Request for Proposals

Provider Directory Services with eHIE Capabilities

Cal eConnect, Inc.

RFP: 2011-011

Posted: May 9, 2011

Table of Contents

I INTRODUCTION

I.A. Purpose

Cal eConnect invites interested and qualified vendors to submit competitive and innovative proposals for the design, development, implementation, operation, and maintenance of a Provider Directory Service with electronic Health Information Exchange (HIE) Capabilities. The purpose of this Request for Proposals (RFP) is to procure the services of a vendor or vendor consortium that will work with Cal eConnect not only to launch, but potentially to sustain its core infrastructure. The contract resulting from the RFP will enable electronic HIE to occur in accordance with the goals and objectives outlined in the Office of the National Coordinator's State Cooperative Agreement program for Health Information Exchange.

The Contractor resulting from this RFP process will provide the following services:

- Design, develop, and implement provider directory services with a technical architecture that is flexible and scalable enough to provide a variety of exchange services or capabilities.
- Design, develop, and implement a suite of exchange services that have the capacity to enable the sharing of electronic lab results and patient care summaries at a minimum. However, other services may be proposed in your response to the RFP.
- Host the provider directory services and work with Cal eConnect to make them available to health care providers across the vast state of California.
- Develop and provide an implementation plan for the administration, operation, and maintenance of the provider directory services and the exchange services infrastructure.
- Operation/Maintenance of the Provider Directory Services is dependent upon deployment capabilities, cost performance, and available resources.

In the remainder of this document, the vendor or vendor consortium is referred to as “Bidder” with regard to procurement-related activities and “Contractor” after contract execution.

I.B. Background

On January 6, 2009, Congress passed the Health Information Technology for Economic and Clinical Health Act (HITECH), a component of the American Recovery and Reinvestment Act (ARRA). The Act authorizes the federal government to develop programs to support the “Meaningful Use” of Electronic Health Records (EHRs) for hospitals and providers and award up to $30 billion in incentives nationally over a ten-year period. One of the Act's core programs funds States and State Designated Entities to support expansion of secure health information exchange (HIE). Secure HIE is necessary to allow eligible hospitals and providers to meet the Center for Medicare and Medicaid Services (CMS) EHR Incentive Program meaningful use requirements, and to improve health care services generally by making more accurate health information safely available at the point of care.

The California Health & Human Services Agency (CHHS) applied for and received a $38.8 million award from the Office of the National Coordinator's (ONC) State HIE Cooperative Agreement program and Cal eConnect is using these funds to expand HIE capacity in

California. California's state governance entity (SGE) for HIE was selected through a CHHS Request for Information process. Cal eConnect is a non-profit public benefit corporation with a diverse 22-member public-private stakeholder board responsible for meeting requirements that CHHS sets forth in its sub grant agreements. Cal eConnect was issued an initial grant agreement with specific milestones and deliverables on April 12, 2010.

While the State Designated Entities (SDEs) and their governance bodies have been created in the context of ARRA/HITECH policy, the expectation is that they will continue to serve their respective communities well beyond the end of the HIE Cooperative Agreement program which ends in February, 2014. As such, the ONC has asked each of the states to develop and present both a short term operational and implementation plan and approaches for long term sustainability. Cal eConnect's HIE Strategic and Operational Plan, and the technical implementation plan, and the sustainability plans can be found at www.caleconnect.org.

The successful Bidder should be familiar with the above referenced plans and be able to propose a market-driven solution to the provider directory services with eHIE capabilities that facilitates, enhances, and advances the goals of State Cooperative Agreement program outlined in HITECH, the Funding Opportunity Announcement, and subsequent program information notices and policy guidance released by ONC related to the utilization of provider directories and the use of Nationwide Health Information Network's Direct standards and protocols. In addition, the vendor should not rely on draft documents developed by Cal eConnect to guide RFP responses.

Through the state cooperative agreement, Cal eConnect is focused on providing services that will enable the trusted exchange of electronic health information regionally and across the state using standard-based components and services. This RFP outlines the scope of work that Cal eConnect would like its strategic business partner to fill as part of the core infrastructure California will provide to the health care market place.

I.C. Reference Documents

Considerable information about Cal eConnect may be found at our web site (http://www.caleconnect.org/). In addition, the following documents provide useful background about Cal eConnect and the State Cooperative Agreement program. *Note: The Bidder should not rely on draft documents produced by Cal eConnect to guide their proposal response.*

California's HIE Strategic and Operational Plans developed by California stakeholders through a State-led process and submitted to ONC on March 31, 2010 as a requirement for funding under the State HIE Cooperative Agreement program. These plans provide a comprehensive approach to addressing the state's HIE needs, while acknowledging California's breadth, diversity, and the complexity of implementing state-level HIE initiatives. These documents provide important definitions and contextual information needed to evaluate the functional requirements outlined in the Technical Implementation Plan. See http://www.caleconnect.org/?page_id=22

The Technical Implementation Plan was completed and submitted in June 2010 by a team of consultants and submitted to CHHS per the cooperative agreement between CHHS, and ONC. The plan outlines the approach for utilizing the agreed-upon framework described in the HIE Strategic and Operational Plans for creating a set of the core services deemed essential in maintaining the integrity and relevance of statewide HIE. The plan acknowledges the dynamic nature of industry standards and federal requirements. See http://www.caleconnect.org/?page_id=23

Draft Technical Specifications for the Core Services were completed in July 2010 by technical consultants for Cal and presented as an addendum to the Technical Implementation Plan. The document eConnect describes high-level draft functional requirements and technical specifications for the Cal eConnect HIE infrastructure. The purpose of the document was to expand the detail provided in The Technical Implementation Plan and inform the Request for Proposals during the contracting process for Core Services. See http://www.caleconnect.org/?page_id=23

ONC Program Information Notice (ONC-HIE-PIN-001) released to states on July 6, 2010, provides recommendations and requirements for the activities of the HIE Cooperative Agreement awardees and identifies key deliverables for which Cal eConnect will be held accountable in 2011. See http://www.caleconnect.org/?page_id=66

I.D. Project Tasks and Deliverables

Based upon funding mandates, Cal eConnect has a very aggressive timeframe for procuring these services and implementing the core infrastructure. The contractor shall present all deliverables in a format approved by Cal eConnect.

Task	Deliverable
Services to be Delivered	
System Design, Development, and Implementation	• Validated Approved Requirements and Technical Specification • Technical Design Document • Draft Application Programming Interface Specifications • Concept of Operations • Test Plan • Cal eConnect Infrastructure Demonstration • Acceptance Testing Report • Implementation Plan • Service Guide • Maintenance Plan •
Hosting and Data Center Operations	• Change Control and Configuration Management • Standard Operating Procedures • Business Continuity and Disaster Recovery Plan
Data Acquisition Strategy and Implementation	• Data Acquisition Plan Document • Completed Data Acquisition per the approved plan and in accordance with project phases
Service Adoption and Utilization	• Service Adoption and Utilization Plan • Completed Implementation Strategy per the approved plan and in accordance with the project phases
Provider Certification and Maintenance	
Reporting and Auditing Services	• Various Standard Reports • Various Ad Hoc Reports

Task	Deliverable
Technical Assistance on Policy Operations Development	• Policy and Compliance Management Plan • Dedicated technical support throughout the policy development life cycle
Fraud Prevention and Monitoring	• Fraud Prevention and Monitoring Plan
Call Center and Data Trading Partner Support	• Help Desk Procedures • Periodic Reports on Call Center Utilization, Quality, and Performance
Billing and Accounts Receivable Services	
Exchange Services Capability	• Laboratory results • Patient care summary • Description of additional value-add services
Contractor Responsibilities	
Contract Management	• Project and Management Plan • Contract Budget Tracking Report • Weekly Project Status and Progress Review • Monthly Project Status and Progress Summary Report • Monthly Financial Management Status Report
Quality Assurance	• Performance Based Services Plan
Compliance with Cal eConnect Procedures	
Electronic Library	
End-of-Contract Transition	• System Transition Plan

While the contract resulting from this RFP will be executed between Cal eConnect and the Contractor for the benefit of data trading partners in California, Cal eConnect is currently in discussions with several other states to develop Memorandums of Understanding which would allow them the option to leverage Cal eConnect's provider directory services infrastructure, once implemented.

I.E. Procurement Authority

Cal eConnect, Inc., is a non-profit public benefit corporation and is the accountable party. Committed to conducting a fair and open procurement, Cal eConnect is directly managing all aspects of the selection process. As such, this is a private sector procurement conducted as described within and in compliance with Cal eConnect's approved Procurement Policy (http://www.caleconnect.org/?page_id=26). All contact shall be with Cal eConnect (see instructions within). Respondents shall not contact California state agencies with regard to this procurement.

While this is a private sector procurement, it is being conducted in support of a cooperative agreement among Cal eConnect, the California Health and Human Services Agency (CHHS), and the Office of the National Coordinator (ONC), and utilizes American Recovery and Reinvestment Act (ARRA) grant funds. As such, Cal eConnect will conduct the procurement in a transparent manner that meets the key needs of Cal eConnect's data trading partners.

Contractor agrees to provide the services resulting from this procurement in a manner that maintains the integrity of the American Recovery and Reinvestment Act of 2009.

II OVERVIEW

II.A. Key Procurement Dates

The following projected timetable is set forth for informational and planning purposes. The dates may change at Cal eConnect's discretion. Bidders are responsible for checking the Cal eConnect website for changes or updates to this timetable and addendums to RFP. All times noted are Pacific Time.

Ref #	Event	Day/Date/Time
1.	RFP posted at www.caleconnect.org	Monday/May 9, 2011
2.	Bidders' Conference Location: TBD (check website for update)	Date & Time: TBD (check website for update)
3.	Non-binding Letters of Intent Due to Cal eConnect RFP Contact noted below (e-mail submissions acceptable)	Friday/ May 20, 2011/ 4:00 PM
4.	Written Questions Due to Cal eConnect RFP Contact noted below (e-mail submissions acceptable)	Friday/ May 27, 2011/ 4:00 PM
5.	Responses to Written Questions Posted at www.caleconnect.org	Friday/ June 3, 2011
6.	Proposals due to Cal eConnect RFP Contact noted below via proposal transmission criteria outlined in section IV.G Proposal Packaging and Delivery	Wednesday/ June 22, 2011/ 4:00 PM
7.	Proposal Review Period	June 22 – July 8, 2011
8.	Oral Presentation/Demonstrations by Invitation Only	July 11 – 15, 2011 Dates and Times: TBD
9.	Presentation of Successful Bidders to Cal eConnect Board of Directors	Friday/ July 22, 2011/ 10:00 AM
10.	Post Notice of Intent to Award	Monday/ August 1, 2011
11.	Desired Contract Execution	Monday/ August 15, 2011

II.B. Contact

This RFP is issued by Cal eConnect. Issuance of this RFP does not constitute a commitment by Cal eConnect to award a contract. The contact person listed below is the sole point of contact relative to this RFP. Any and all notices pertaining to this RFP should be directed in writing to Gwyn Jackson at gjackson@caleconnect.org. Include “RFP-2011-011” in the subject heading.

Non-binding letters of intent, questions related to the RFP, and final Proposals are due to Ms. Jackson at the following address per the above referenced timeline:

Cal eConnect
Attn: Gwyn Jackson
1900 Powell Street, Suite 1000
Emeryville, CA 94608
(916) 308-7064

After issuance of this RFP, no contact will be allowed between Bidders and Cal eConnect’s employees, procurement consultants or contractors, board members, steering committee members, or RFP evaluators. All contact and communications related to this RFP and the products and services Cal eConnect seeks to procure must be directed to the Cal eConnect contact person named above. Any other such contact may disqualify a Bidder from further consideration. Requests for clarification by Bidders will be allowed provided that such requests are made through the above contact.

II.C. Proposal Checklist

The following checklist is provided to assist Bidders with the assembly of their proposals. It is the Bidder's responsibility to verify their proposal complies with the content and packaging requirements documented in Section IV, Proposal Submission Requirements.

☐ The following items are submitted in a sealed package

☐ A. Mandatory Submittals
☐ 1. Transmittal Letter
☐ 2. Minimum Corporate Experience Summary Form (Attachment A)
☐ 3. Corporate Experience Client Reference Form (Attachment B)
☐ 4. Project Team Form (Attachment C)
☐ 5. Minimum Staff Experience Form (Attachment D)
☐ 6. Pre-Existing Software Form (Attachment E)

☐ B. Company Background and Experience
☐ 1. Corporate Qualifications
☐ 2. Staff Qualifications

☐ C. Proposed Approach to the Scope of Work
☐ 1. Services to be Delivered
☐ 2. Solution to Functional and Technical Requirements
☐ 3. Contractor Responsibilities

☐ D. Use Case Responses

☐ E. Optional Value-Add Exchange Services and Approach to Sustainability

☐ F. Compact disk with electronic version of the proposal, in Microsoft Office 2010 or Acrobat Reader 8.0.

☐ No cost information is submitted in package 1

☐ The submission is clearly marked "RFP-2011-011"

☐ The following items are submitted in a ***separately*** sealed package

☐ A. Cost Proposal for Mandatory Services

☐ B. Cost Proposal for Optional Services

☐ C. Compact disk with cost proposal, completed cost proposal Excel workbook, completed cost proposal optional services Excel workbook, and additional cost proposal information, in Microsoft Office 2010 or Acrobat Reader 8.0.

II.D. Examination of All Requirements

Bidders should thoroughly examine this document and be knowledgeable of the scope of work required. Responses must be based solely on the information and materials contained in the RFP, as well as any amendments or other subsequent written materials issued by Cal eConnect, and any written answers Cal eConnect provides in response to Bidders' written questions. Bidders are to disregard anything else, including draft material they may have received, any newspaper advertisements or articles they may have read, and any oral representations made.

If a Bidder fails to notify Cal eConnect of an error in the RFP which has been identified, the submission of the response is at the Bidder's own risk. If awarded the contract, the Bidder will not be entitled to additional compensation or time due to the error or its correction.

Cal eConnect, in its discretion, may refuse to accept a response for failure to furnish all required information or to follow the format specified in this RFP.

II.E. Amendments to the RFP

Cancellation or Amendment to the RFP. Cal eConnect may cancel or amend the RFP and Notice of Amendment or Cancellation will be sent:

- To Bidders who submitted an Intent to Bid if the amendment or cancellation occurs prior to submission of the RFP response;
- To Bidders who submitted an RFP response if the amendment or cancellation occurs after submission; and
- To Finalists if the amendment or cancellation occurs after Finalists have been identified.

II.F. Intent to Bid

Bidders must submit a written Intent to Bid via email to Cal eConnect by the date and time specified in Section II.A, Key Procurement Dates in order to receive any further communications regarding this RFP. If a written Intent to Bid is not sent, a proposal may still be submitted; however, any further notices issued by Cal eConnect will only be sent to Bidders that have an Intent to Bid on file. All Vendors are expected to access notices and amendments issued by Cal eConnect regarding this solicitation on Cal eConnect's website (www.caleconnect.org) under "Opportunities" / "Contracts" up to the due date for RFP responses. After the RFP response due date, notices and amendments will be sent only to those Bidders who have submitted a proposal. After Finalists have been identified, notices and amendments will only be sent to the relevant Finalists.

In order to facilitate direct communications between potential Bidders who may wish to collaborate, Cal eConnect will send a list of Bidders who have submitted an Intent to Bid and a list of Bidders who attend the Bidders' Conference to those Bidders that submit an Intent to Bid.

II.G. Written Questions

Questions regarding this RFP must be submitted in writing via email to the Cal eConnect contact person specified in Section II.B, Contact, by the date and time specified in Section II.A, Key Procurement Dates. All Bidders with a written Intent to Bid on file will receive a copy of all written questions and answers that Cal eConnect has addressed.

II.H. Bid Consideration

In consideration for being permitted to submit a proposal, the Bidder agrees that:

1. Any and all information provided to Bidders by Cal eConnect is proprietary information and is to be used solely for the purpose of responding to this RFP.
2. Bidder responses will be the sole property of Cal eConnect.
3. Cal eConnect is not liable for any costs incurred by a Bidder in preparing, submitting, or otherwise participating in a response to this RFP.
4. The response received from the successful Bidder within this RFP, either in whole or in part, at Cal eConnect's option, will become part of the contract between Cal eConnect and the Bidder.
5. By issuance of this RFP, Cal eConnect is not obligated to award a contract.

II.I. Confidentiality of Bidder's Responses

Stakeholder observers will be engaged in the review process as members of the Evaluation Committee and will have access to Bidder responses solely for the purpose of participating in the review. Members of the Evaluation Committee will complete a conflict of interest form and sign a non-disclosure agreement with Cal eConnect for the purpose of reviewing and evaluating proposals. No competing Bidders will be allowed to participate in this stakeholder review process. Cal eConnect will not release copies of Bidders' responses to any private parties outside of the review process during the timeframe of the procurement (i.e., until the contract resulting from this procurement is executed). Bidders who are concerned with stakeholder participation in the review process should not submit a response to this RFP.

Cal eConnect shall, upon request, make available to CHHS and/or the Office of National Coordinator for Health Information Technology of the U.S. Department of Health and Human Services ("HHS"), pre-award review, procurement documents (e.g., requests for proposals or invitations for bids, Bidders' responses), independent cost estimates, or other materials or tools. In addition, Cal eConnect reserves the right to summarize components of the responses and make the information available in order to provide transparency into the selection process.

Cal eConnect may make available to private individuals or organizations copies of Bidders' responses in compliance with the grant agreement(s) that provide funds for the executed contract. Under no circumstance will Cal eConnect be liable to the Contractor or to any other person or entity for disclosing any portion of Bidder's submissions in response to this RFP, including those portions Bidder has asserted are confidential.

II.J. Rejection of Responses

Cal eConnect reserves the right to reject any response which is conditional or incomplete, or contains any material deviations. Any provisions of this document which are identified as mandatory requirements must be met. In the interest of promoting competition, Cal eConnect may allow a Bidder to correct a deficiency related to any requirement upon Cal eConnect's written request. If all Bidders fail to meet a mandatory requirement, Cal eConnect reserves the right to continue evaluation of the proposals and select the response which most closely meets the requirements specified in this RFP. In the event that Cal eConnect determines proposals from all Bidders contain material deviations, Cal eConnect reserves the right to declare the proposals to be draft proposals. Bidders may not protest Cal eConnect's determination that all bids have material deviations.

II.K. Nonmaterial Deviation

Cal eConnect may waive any nonmaterial deviation in a proposal. The determination of what constitutes a nonmaterial deviation is at the sole discretion of Cal eConnect. Cal eConnect's waiver of a nonmaterial deviation does not modify the RFP requirements or excuse the proposing Bidder from full compliance with the contract's requirements.

II.L. Contract Execution and Duration

The Cal eConnect Chief Executive Officer (CEO) or designee will make the final determination of the contract award, subject to Board of Directors approval. In making this determination, the Cal eConnect CEO or designee will be assisted by an Evaluation Committee.

Cal eConnect reserves the right to cancel any and all elements of this procurement or rescind an announced award at any time up to and including execution of the actual contract.

The duration of this contract will be a **minimum of two years, with options for three, one-year extensions,** but will be adjusted based in part upon RFP responses from Bidders, balanced with Cal eConnect and ONC mandates.

III SCOPE OF WORK

The next three sub-sections: A) Services to be Delivered, B) Functional and Technical Requirements of the System, and C) Contractor Responsibilities describe Cal eConnect expectations of the vendor and Scope of Work to be performed including anticipated deliverables. Section IV outlines the proposal submission criteria. Please base proposal on the Scope of Work provided herein.

III.A. Services to be Delivered

III.A.1 System Design, Development, and Implementation

Task 1. Functional, Technical, and Performance Requirements Validation

Refine the functional, technical, and performance requirements defined in the Functional Requirements and Technical Specifications so that they accurately reflect the capabilities of the proposed solution and may be used as the basis of acceptance criteria for that solution. The final requirements deliverables must be approved by Cal eConnect and subsequent modifications or changes must also be approved.

Deliverable: Validated Approved Requirements and Technical Specification

Task 2. Design

Contractor will design the solution to meet the validated requirements from Task 1. Deliverables resulting from this task will be used to validate that the design meets the requirements. Contractor will walk Cal eConnect project staff through the design documents and describe how the design meets the requirements. During this task, Cal eConnect will identify the Phase 1 users. Contractor will engage end-users in the design and development process for external facing user interfaces (such as Individual Providers maintaining their information).

Deliverable: Technical Design Document showing how requirements will be met by the solution, including:

- Describe architecture of technical solution, including all major components and interfaces among them, as well as interfaces to external clients/users of the solution (the technology stack)
- Describe custom development required (as opposed to use of pre-existing Contractor, open source, or other licensed third-party software, henceforth, “Pre-existing Software”) and design of custom-developed software
- Describe configuration required for Pre-existing Software and how that configuration meets design requirements

Deliverable: Draft Application Programming Interface Specifications for all APIs to be used by external data trading partners as they develop programmatic interfaces to the infrastructure

- Describe specifications of all APIs
- Describe technical specifications

Task 3. Development

Contractor will develop and configure the solution in compliance with the approved Technical Design Document deliverable (Task 2) to meet the Validated Approved Requirements (Task 1). The Contractor's development team will verify that Cal eConnect requirements, as documented in the Validated Approved Requirements Deliverable, are met and will work to establish a Concept of Operations with use cases based on the developed solution.

Deliverable: Concept of Operations with use cases, including:

- i. System Overview
- ii. Scope Description
- iii. Operational Needs
- iv. User-Oriented Operational Description
- v. Operational and Support Environments
- vi. Operational Scenarios

Task 4. Unit and Integrated System Testing

The Contractor shall be responsible for conducting Unit and Integrated System Testing and will:

1) Develop a Test Plan that includes:
    - a. Approach Planned
        - i. Documenting the Processes & Procedure
        - ii. Use of Tools and Tool Techniques
        - iii. Incident Management
        - iv. Identifying, Collecting, Installing, and Managing Test Data
        - v. Performing Backup and Restore
    - b. Identification of Roles and Responsibilities
    - c. Tester Training
    - d. Description of Test Environment(s)
    - e. Contractor Test Environment Management
    - f. Definition of Testing Metrics including Incident and Script level metrics
    - g. Test Results documentation and tracking
    - h. Test script development and approval process
    - i. Acceptance criteria for Full System Acceptance
2) Install, setup, support, upgrade, and maintain, all software, tools, and products required for the Provider Directory Services with eHIE Capabilities System Testing
3) With Cal eConnect and Data Trading Partner support, connect the Provider Directory testing environment to test environments for the required external system interfaces, or demonstrate connectivity for those interfaced systems without dedicated test environments
4) Tune and/or configure testing environment hardware, software, tools, and products to achieve required functionality
5) Set up the Test Environment with a fully functional Provider Directory Services with eHIE Capabilities System
6) Ensure availability of the Testing Environment during testing periods

7) Provide resources to write and execute all System Testing test scripts
8) Develop Test Scripts for each function with expected results, prior to beginning any System Testing
9) Update Technical Documentation as needed:
    a. Technical Design Document
    b. Draft Application Programming Interface Specifications
    c. Concept of Operations
10) Chair testing status meetings with both Contactor's and Cal eConnect's staff
11) Document Test Results
12) Provide Daily Testing Status Reports including Testing Metrics and Incidents as defined in the Test Plan
13) Identify, Collect, Install, and Manage pre-conditioned Test Data
14) Provide technical support staff to resolve reported Incidents and issues
15) After completion of Unit and Integrated System Testing, provide a demonstration of the completed system to Cal eConnect

Deliverable: Test Plan

Deliverable: Cal eConnect Infrastructure Demonstration, including:

i. Demonstrate solution
ii. Demonstrate compliance with security requirements
iii. Demonstrate that the solution meets acceptance criteria

Task 5. User Acceptance Testing

In accordance with the approved Test Plan, Cal eConnect will perform initial acceptance testing of the solution to verify that the solution meets minimum acceptance criteria. This will be followed by Phase 1 users who will perform the UAT scripts and record the results.

Deliverable: Acceptance Testing Report that documents the compliance of the solution with each acceptance-testing criterion

Task 6. Implementation

Contractor will develop an Implementation Plan for deploying the solution to users in Phases 1 through 3 (See Section III.D, Phasing of Deliverables). Contractor will develop a Service Guide that gives data trading partners the information they need to connect to and use the infrastructure. Contractor will initiate a "participant testing/certification environment" that mimics the response from the production system for data trading partners to test their interfaces. Contractor will also develop a maintenance plan that describes how the solution and documentation will be maintained to incorporate changing federal and state standards, new services or features, and other changes. Contractor will implement all services required to support the security features of the solution (including user certification and granting of digital certificates).

Deliverable: Implementation Plan

Deliverable: Service Guide that gives provider organizations the information and instructions they need to connect to and use the infrastructure

Deliverable: Maintenance Plan

i. Describes a formal change management process, to ensure that changes introduced are in a controlled and coordinated manner and that load testing has been performed
ii. Describes how new services or features will be incorporated
iii. Describes how design documents and API's will be maintained throughout the life of the contract so that the most current version is reflected in the documentation
iv. Includes a Document Management Plan that describes how the documents will be kept up to date

III.A.2 Hosting and Data Center Operations

Contractor will host the Cal eConnect Infrastructure as a web-based solution with 99.999%, 24x7x365 availability to users, whether through programmatic interfaces or direct user interfaces. Contractor's hosting facility will comply with Health Insurance Portability and Accountability Act (HIPAA) security control requirements. The Contractor will provide the following hosting and security services:

1) Provide and manage a secure hosting facility for the following system environments, to include:
    a. Production environment
    b. Test Harness environment
    c. Development and testing environment
    d. Staging/preproduction environment
    e. Upgrade and updates for all environments, including operating systems
2) Provide dedicated server hardware and network equipment (i.e. routers, switchers, firewalls, load balancers, etc.) to support federated hosting environment and services to accommodate:
    a. 500,000 Individual Providers
    b. 60,000 Entities
    c. 120,000 client applications
3) Provide internet connections and redundant network bandwidth to support federated hosting environment that meets the performance requirements documented in Exhibit C.
4) Conduct administration and operations for federated hosting environment and Provider Directory Services with eHIE Capabilities Infrastructure
5) Provide maintenance and support of the federated hosting environment and Provider Directory Services with eHIE Capabilities Infrastructure (operating systems, infrastructure, servers, applications), to include, but not limited to:
    a. Implement approved infrastructure configuration
    b. Establish and maintain configuration and system parameters in a consistent manner across all environments
    c. Establish and maintain Provider Directory Services with eHIE Capabilities Infrastructure applications
    d. Perform authorized system changes
    e. Execute environment creation, upgrade and refresh

   f. Coordinate impacts of all infrastructure maintenance with PMO adhering to the Change Control and Configuration Management procedures

6) Environment must meet HIPAA security control requirements:
   a. Physical Safeguards:
      i. Facility Access Controls
      ii. Workstation Use
      iii. Workstation Security
      iv. Device and Media Controls
   b. Administrative Procedures:
      i. Security Management Process
      ii. Assigned Security Responsibility
      iii. Workforce Security
      iv. Information Access Management
      v. Security Awareness and Training
      vi. Security Incident Procedures
      vii. Contingency Planning
      viii. Evaluation
      ix. Business Associate Contracts and Other Arrangements
   c. Technical Safeguards:
      i. Access Controls
      ii. Audit Controls
      iii. Integrity
      iv. Person or Entity Authentication
      v. Transmission Security
7) Define, document, and maintain Change Control and Configuration Management procedures for the Provider Directory Services with eHIE Capabilities Infrastructure and hosted environment
8) Define, document, and maintain standard operating procedures for maintaining specified service levels and measuring performance
9) Define, document, and maintain Business Continuity and Disaster Recovery procedures for recovering the system to specified service levels in the in the event of a disruptive event
10) Provide availability guarantees based on performance service level requirements in Exhibit C

Deliverable: Change Control and Configuration Management procedures

Deliverable: Standard Operating Procedures for maintaining specified service levels and measuring performance

Deliverable: Business Continuity and Disaster Recovery Plan, which will document procedures for recovering the system to specified service levels in the in the event of a disruptive event

III.A.3 Data Acquisition Strategy and Implementation

Contractor will acquire provider data from existing sources to populate the Provider Directory and will perform the following tasks:

1. Identify provider data needed to populate the Provider Directory
2. Identify sources of collecting provider data
3. Work with source organizations to gain one-time and ongoing access to provider data
4. Load provider data into the Provider Directory
5. Maintain and improve provider data on an ongoing basis

Deliverable: Data Acquisition Plan Document

Deliverable: Complete Data Acquisition per the approved plan and in accordance with the project phases

III.A.4 Service Adoption and Utilization

Contractor will develop a Service Adoption and Utilization Plan that describes how the Bidder will encourage adoption and use of the Provider Directory. Contractor will implement the Plan at the direction of Cal eConnect.

1) Develop a Service Adoption and Utilization Plan to encourage adoption by users that may include development of incentives or benefits for participation in directory
2) Set adoption objectives
3) Identify barriers to adoption
4) Work with Cal eConnect to identify strategies for increasing adoption
    a. Reduction of barriers to adoption
    b. Incentives or benefits for adoption
    c. Encourage consistent implementation of Cal eConnect supported messaging standards
5) Develop action plans for approved strategies
6) Implement the approved action plans, at the direction of Cal eConnect
7) Conduct periodic statewide surveys regarding the adoption of the Provider Directory

Deliverable: Service Adoption and Utilization Plan for encouraging adoption of the Provider Directory Services with eHIE Capabilities by users

Deliverable: Complete Implementation Strategy per the approved plan and in accordance with the project phases

III.A.5 Provider Certification and Maintenance (Verification and Validation)

Contractor shall be responsible for providing, in addition to the technology solution described in Section III.B Functional and Technical Requirements of the System, the following services throughout the digital certificate lifecycle based on Cal eConnect policies:

- On-boarding provider entities and individuals
- Certification of provider entities
- Certification of individual providers
- Issuing level 3 digital certificates
- Periodic recertification of provider entities and individuals

- Automation of the certification and recertification process utilizing information available from:
    - California government agencies
    - CMS and its agencies
    - Medical Associations
- Off-boarding of provider entities and individuals
- Management of revocation lists for digital certificates
- Renewal of expired certificates
- Primary source verification of licensed individuals
- Managing and improving the quality of data in the system

Throughout the digital certificate lifecycle, specific service requirements for Entities, Nodes, and Individual Providers are:

1) Entities (Root, Tree, and Leaf)
    a. Entry and maintenance of demographic information (via API or Web UI)
        i. By the entity
        ii. By a proxy for the entity (who conforms to the Cal eConnect standards for a proxy)
        iii. By Cal eConnect at request of the entity
        iv. By Cal eConnect or its designated proxies who conform to the Cal eConnect standards for a proxy
    b. Cal eConnect Level III credentialing (verification of entity consistent with NIST Level III)
        i. Comparison to state and federal resources that have information on entities
        ii. In person attestation if required
    c. Equivalent credentialing by the State of California
    d. Equivalent credentialing by the Federal Government
    e. Equivalent credentialing by Cal eConnect recognized Certificate Authority (CA) agencies following protocols accepted by Cal eConnect
    f. Secure issuance and distribution of Level 3 (Class 3) digital certificate to Entity
    g. Activation, recertification, and deactivation of entities / digital certificates
2) Nodes
    a. Entry and maintenance of node information (via API or Web User Interface)
        i. By the entity
        ii. By a proxy for the entity (who conforms to the Cal eConnect standards for a proxy)
        iii. By Cal eConnect at request of the entity
        iv. Selected from certified Health Information Services Provider (HISP) or HIE entity nodes
    b. Validation of node capability via Test Harness
    c. Validation of node support for Services Registry entries via Test Harness
    d. Entry of Test Harness key by entity, proxy, or Cal eConnect
    e. Secure issuance and distribution of Digital Certificate for node if not inherited from Entity leaf

f. Maintenance of node information
g. Revocation of node if required by policy

3) Individual Providers (non-licensed) – responsibility of the declaring Entity
    a. Entry and maintenance of demographic information and Digital Certificate (Level 3) (via API, batch, or Web UI)
        i. By the entity
        ii. By a proxy for the entity (who conforms to the Cal eConnect standards for a proxy)
    b. Validation of naming conventions to avoid confusion during search
    c. Activation and deactivation of Individual Providers (based on Cal eConnect policy)
    d. Revocation if necessary
4) Individual Providers (licensed)
    a. Entry and maintenance of demographic information (via API, batch, or Web UI)
        i. By the Entity as a proxy for the individual providers
        ii. By a proxy for the individual provider (who conforms to the Cal eConnect standards for a proxy)
        iii. By Cal eConnect at request of the individual provider
        iv. By Cal eConnect or its designated proxies who conform to the Cal eConnect standards for a proxy
    b. Cal eConnect Level III credentialing (verification of individual consistent with NIST Level III)
        i. Comparison to state and federal resources that have information on entities
        ii. In person attestation if required
    c. Equivalent credentialing by the proxy Entity
    d. Equivalent credentialing by the State of California
    e. Equivalent credentialing by the Federal Government
    f. Equivalent credentialing by Cal eConnect recognized CA agencies following protocols accepted by Cal eConnect
    g. Secure issuance and distribution of Level 3 (Class 3) digital certificate to Entity
    h. Activation, recertification, and deactivation of entities / digital certificates
    i. Initial Primary Source validation of documents and attestation as required by California provider organizations (certificate verification organization (CVO) capability)
    j. Declaration of relationship with Entities
        i. Via proxy Entity (declares both side of relationship)
        ii. Via Individual or Entity and confirmed by the other (like social networking)
        iii. Revoked by either side
    k. Periodic review of credentials as they are renewed or based on Cal eConnect policy
    l. Management of permission to release to third parties via Individual (Web User Interface) or on request by Cal eConnect (Contractor).

III.A.6 Reporting and Auditing Services

Cal eConnect will need the ability to analyze, audit, and report upon the contents and utilization of the Cal eConnect infrastructure components. This reporting and auditing capability will be available to internal Cal eConnect users, and will not be available to external users. The Contractor will provide a centralized capability that provides a wide range of querying, analytical, reporting, and auditing functions across all of the components of the infrastructure. The purpose of this capability will be to allow Cal eConnect to periodically assess the level of usage of the infrastructure, monitor its performance, gauge the resources required to operate the infrastructure, and retrieve information on specific transactions for authorized auditing purposes. The general features of the reporting/auditing capability should include:

- A flexible reporting architecture
- The availability of standard (canned) reports
- The ability to specify *ad hoc* reports, including through user-friendly forms-based report writers, as well as through direct access to relational database structures via SQL
- The reporting and auditing functions should not impact the performance or security of the infrastructure

Report Contents. The reporting capability should have the capability to generate reports containing the following types of information at a minimum:

- System performance/response time by Core Service and transaction type
- Number of registered Entities, Nodes, and Individual Providers
- Number of transactions by Core Service and transaction type
- Number of transactions by Entity, Individual Provider, and transaction type
- Number of new certificates issued, by Entity or Individual Provider
- Number of Exchange Service translations performed, by protocol
- Number of new enrollments by Entity and Individual Provider in a given month, grouped by region, county, type of entity
- Costs associated with on-boarding Entities, Nodes, and Individual Providers, including costs for certification, private-key distribution, and technical support
- Costs associated with ongoing customer support following initial on-boarding, including technical support and end-user customer support
- Error reports, at the level of specificity necessary to research and resolve the error
- Financial transactions count and dollar amounts
- Customer transactions count and dollar amounts
- Accounts receivable subsidiary ledger account balances (including customers)

In addition to generating static reports on demand, the reporting capability shall also provide an online “dashboard” that displays current statistics regarding many of the parameters listed above. The purposes of this dashboard shall be to provide a snapshot to Cal eConnect personnel of the current state of the infrastructure and any notable trends in its use or growth.

Report content shall include tabular and graphical formatting of data. Dynamic “OLAP” capabilities are not required in the initial version of this capability, although reports should be accessible and viewable online, as well as printable. The report capability should also be able to export specified data via CSV files or similar formats for processing within other database or analytical tools.

III.A.7 Technical Assistance on Policy Operations Development

A major success factor of the to-be solution is a comprehensive yet transparent realization of Cal eConnect's Policies and Procedures related to the adoption and meaningful use of the Infrastructure across California. Cal eConnect shall be the sole authoritative source of all of the Network's Policies and Procedures. Working with Cal eConnect, its Policy Advisory Group and other designees as indicated by Cal eConnect, the Contractor will be required to support and provide technical input to the development, execution and monitoring of compliance to the Policies and Procedures as formally approved by Cal eConnect.

Contractor will provide technical assistance on policy operations development related to on-boarding and off-boarding of Entities and Individual Providers. For example, policies related to:

1. Use of the Provider Directory Services with eHIE Capabilities
2. Managing confidential information (such as provider credentials)
3. Transactions requiring a Business Associate Agreement
4. Data sharing and data availability agreements
5. Other policies identified by Cal eConnect

Contractor will develop a Policy and Compliance Management Plan based on policies set by Cal eConnect. This plan will include detailed standard operating procedures on how Cal eConnect's policies are supported by the operational procedures of the various functionalities of the system as well as change management procedures to facilitate the implementation of new or modified Policy.

Deliverable: Policy and Compliance Management Plan related to on-boarding and off-boarding of Entities and Individual Providers

Deliverable: Dedicated technical support throughout the policy development life cycle

III.A.8 Fraud Prevention and Monitoring

Contractor will provide fraud prevention plan and strategy to proactively identify Provider Directory Service transactions that may be fraudulent. Contractor will provide the following fraud management services:

1) Assess fraud risks
    a. Conduct a one-time assessment to gauge the extent and types of fraudulent activities. For example:
        i. Use of false names, social security numbers, or other information
        ii. Use of compromised digital certificate
        iii. Use of compromised Node
        iv. Collusion among Entities and/or Individual Providers
        v. Access to sensitive information by unauthorized Entities, Individual Providers, Contractor personnel, Cal eConnect personnel, or others
    b. Develop recommendations (people, process, and technology) for ways to prevent and detect fraud

   c. Document findings and recommendations in a Fraud Prevention and Monitoring Plan

2) Develop and test approved fraud prevention strategies
3) Develop and test approved fraud detection strategies to proactively identify transactions that may be fraudulent
4) Develop and test procedures to resolve and escalate detected instances of fraud in compliance with the Fraud Prevention and Monitoring Plan

Deliverable: Fraud Prevention and Monitoring Plan that identifies:

i. Assessed fraud risks
ii. Fraud prevention strategies
iii. Fraud monitoring and detection strategies
iv. Fraud resolution procedures

III.A.9 Call Center and Data Trading Partner Support

Contractor will provide and staff a toll-free call center to answer users' questions and resolve problems. The call center should be available twenty-four (24) hours per day, seven (7) days per week. The Contractor will provide the following services in compliance with the performance requirements in Exhibit C.

1) The Contractor shall provide and maintain a toll-free call center that is available twenty-four (24) hours per day, seven (7) days per week.
2) The Contractor shall provide call center support for a user who wishes to enter or update information.
3) The Contractor shall provide call center support for a user during the credentialing process.
4) The Contractor shall provide call center support for a user during activation, recertification, and deactivation of digital certificates.
5) The Contractor shall provide call center support for a user who wishes to validate a Node's capability via the Test Harness.
6) The Contractor shall provide call center support for a user who wishes to use the Exchange Services.
7) The Contractor shall provide call center support for a user utilizing the Provider Directory Services with eHIE Capabilities system.
8) The Contractor shall provide call center support for a user to report a lost or compromised digital certificate.
9) The Contractor shall provide call center support for a user to report unauthorized digital certificate use and/or fraud.
10) The Contractor shall provide call center support for a user who wishes to open a claim for a disputed transaction (e.g., billing transaction).
11) The Contractor shall create and maintain comprehensive Help Desk procedures, quick guides and services including processes to publish, record, track and search help desk support service requests through initiation, response, escalation, resolution, and closure.
12) The Contractor shall provide escalation procedures appropriate to the Priority Levels described in Exhibit C.

13) Contractor shall provide call center services in compliance with the performance measures listed in Exhibit C.

Deliverable: Help Desk Procedures that describe processes to publish, record, track and search help desk support service requests through initiation, response, escalation, resolution, and closure

Deliverable: Periodic Reports on Call Center Utilization, Quality, and Performance based on approved metrics and standards.

III.A.10 Billing and Accounts Receivable Services

Contractor will perform billing and accounts receivable services on behalf of Cal eConnect for all functions of the Cal eConnect Infrastructure that require payment of subscription, transaction, or other fees on the part of data trading partners, including:

- Capture and track customer billable activities
- Issue invoices to customers
- Provide monthly statements to customers
- Record accounts receivable transactions to Generally Accepted Accounting Principles-compliant accounts
- Maintain customer account balances in an accounts receivable subsidiary ledger
- Perform collections activities, including issuing dunning notices, making telephone calls, and other activities required to collect on delinquent receivables
- Record cashiering transactions
- Make available financial data (transaction counts and dollar amounts, customer counts and dollar amounts, and balances) to Cal eConnect on a weekly basis, and as requested
- Provide customer support related to billing and payment activities
- Provide dispute-resolution processes and services related to billing and payment, per policies agreed upon with Cal eConnect

III.A.11 Exchange Services Capability

Exchange Services are designed to encourage the early adoption and continued use of the Cal eConnect Trust Framework – including the Provider Directory Services, Messaging Format, and Authorization Infrastructure. The Contractor will provide exchange services for the following message translations:

Message Translations	From Protocol	To Protocol
Patient Care Summaries	CCD	CCR
Laboratory Results	TBD	TBD

Specific functional and technical requirements for the required exchange services are described in Section III.B.3.d.

Contractor shall provide:

1) The overall framework for the Exchange Services
2) Messaging framework access to the services
3) Ability for the services to “proxy” for a sender or consumer
4) User Interface to establish new service and maintain existing services
5) Logging of all transactions
6) Test fixtures to allow Exchange Services users to test by sending to and receiving from Exchange Services along with analysis of the compliance of the users messages and payload

Cal eConnect prefers that the Exchange Services be an open source component, available for multiple parties (e.g. HIEs and other states) to adopt the technology and develop translation services to be shared.

Optional Value-Add Services

Cal eConnect believes that additional, value-added Exchange Services that leverage the Provider Directory Service infrastructure are critical to the success of developing a successful sustainability model. As such, Bidders are encouraged to develop a sustainability approach that includes both descriptions and costing of a portfolio of proposed value-added Exchange Services. Bidder response requirements for these optional services are described in Section IV.E, Optional Value-Add Exchange Services and Approach to Sustainability.

Note: The description and cost data of any additional, value-add Exchange Services proposed is OPTIONAL and will NOT be scored as part of Bidders’ proposals. However, the data and sustainability approach will be considered and scored as part of the final review of Finalists who have been selected for the interview process.

III.B. Functional and Technical Requirements of the System

III.B.1 Overview

Given the dynamic environment of health information exchange today, it is imperative to provide a dynamic solution that is flexible and scalable. Adaptability is crucial in successfully responding to evolving policy frameworks and interoperability standards being developed nationally and in the State of California.

As stated in the California HIT Strategic and Operational Plans, as well as the drafted Cal eConnect HIE Implementation Plan, the technology strategy for statewide services should be focused on supporting meaningful use criteria and must include the following key components:

1. Architectural design of the statewide services is service-oriented, with services implemented as Web services
2. The strategy includes technical specifications and software components required for meaningful use
3. Services should be separated into:
    a. infrastructure components that establish trust through secure, encrypted and reliable exchange of health information over the internet, and
    b. optional value-add services that enable higher-level business processes
4. Policy must inform the development of the messaging framework and trust framework specifications
5. The infrastructure components implement the messaging framework and trust framework specifications
6. The messaging and trust framework for the statewide services must be consistent with the transport standards and security standards identified in the IFR
7. The services and standards developed for NwHIN Exchange should inform the development of the statewide infrastructure and be utilized or leveraged where possible

Cal eConnect's expectation is that the successful Bidder will incorporate the current standards and interoperability requirements being established by the ONC. The Provider Directory Service resulting from this RFP is intended to serve as California's core technical infrastructure for eHealth information exchange at a statewide level. The core consists of the following components:

- Entity Level Provider Directory (ELPD)
- Individual Level Provider Directory (ILPD)
- Services Registry (SR)
- Complex ELPD, ILPD, SR Relationship Support
- Messaging Framework
- Authorization Framework
- Cal eConnect Entity and Node
- Exchange Services
- Test Framework

The following section describes the functional requirements for these components, each of which should be addressed in the submission response.

Exhibit B has more detailed technical criteria, which are intended to serve only as a guide to understanding the functional requirements.

III.B.2 Entity-Centric Business Services: Entity Level Provider Directory Service; Individual Level Provider Directory Service and Service Registry

III.B.2.a Entity Level Provider Directory (ELPD) Service

Description: The Entity Level Provider Directory (ELPD) is a secure repository of information specific to entities and nodes that participate in the Cal eConnect Infrastructure. Key to the repository is a web service API that allows "read" &" write" access, as well as a web browser interface for reviewing information related to Entities. For further information see Exhibit B.

No.	CRITICAL FUNCTIONS
ELPD-A	**Entities to be represented in the ELPD:**
	• HIEs, HIOs, HISPs
	• Hospitals / IDNs
	• Clinics
	• Physician offices / Groups
	• State and Federal health agencies
	• Clinical laboratories
	• Pharmacies / Pharmacy networks
	• Imaging centers
	• Health plans (including Medi-Cal, Medicare)
	• Health centers and FQHCs
	• Transaction intermediaries
	• Nursing homes
	• Home health agencies
	• Professional organizations
	• Rehabilitation facilities
	• Mental health facilities
	• Long term care facilities
	• Hospice
	• HME/DME providers
	• Other Business Associates
	• Personal health records/repositories
ELPD-1	Provide discovery of Entities and Nodes in support of the following Messaging and Authorization models: NwHIN Direct, NwHIN Exchange, Cal eConnect (i.e., as described herein)
ELPD-2	Support the certification and registration of all of the Entity types that may be engaged in health information exchange in California

No.	CRITICAL FUNCTIONS
ELPD-3	Represent Entities at various organizational levels, from high-level corporate entities to individual health care facilities
ELPD-4	Allow each Entity to be associated with one or more Nodes that provide health information exchange services for the Entity
ELPD-5	Represent the health information exchange capabilities of each Node (including the transactions it supports and the technical specifications of the transport, security, and message-formatting methods for each transaction type)
ELPD-6	Include for each node the electronic addressing information needed to send information to the Node in the context of a specific type of transaction
ELPD-7	Be highly secure and impervious to internet-based break-ins, identity spoofing, or denial of service attacks
ELPD-8	Provide both a programmatic API based on the Messaging and Authorization Frameworks described in this document, as well as a highly secure browser-based interface for direct user interaction.
ELPD-9	Require 2-factor authentication for access to the ELPD via the browser-based interface
ELPD-10	Support searching for Entities by a variety of attributes, including name, address, Entity type, NPI, tax ID, etc.)
ELPD- 11	Provide trusted, up-to-date information regarding each registered Entity's and Node's standing in the Cal eConnect Infrastructure, i.e. whether it is certified to conduct transactions
ELPD-12	Provide trusted, up-to-date information regarding each registered Entity's and Node's digital credentials, i.e. whether its digital certificate is valid or has been revoked
ELPD-13	Associate each registered Entity and Node with an X.509 class-3 digital certificate that has been signed by an authorized certificate authority
ELPD-14	Support distribution and federation of service instances to ensure acceptable performance and to allow local management within designated jurisdictions (e.g., states)
ELPD-15	Meet performance requirements
ELPD-16	All user-interface components shall be designed to maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.

No.	CRITICAL FUNCTIONS
ELPD-17	All application programming interfaces shall be designed to minimize the level of effort required on the part of California stakeholders and their H.I.T. vendors to integrate their solutions with the Cal eConnect infrastructure, consistent with the functional and technical requirements of these APIs

III.B.2.b Individual Level Provider Directory (ILPD) Service

Description: The Individual Level Provider Directory (ILPD) is a secure directory of information about providers who participate in the Cal eConnect Infrastructure. The ILPD provides search functions that enable the discovery and lookup of provider information. The ILPD also specifies the Entity or Entities with whom providers are associated. This enables client applications to retrieve relevant information from the ELPD as needed to facilitate the exchange of HIE transactions with the providers. Information can be read or written to the ILPD via a web services API or web browser interface. For further information see Exhibit B.

No.	CRITICAL FUNCTIONS
ILPD-A	**Types of providers to be represented in the ILPD:**
	• Medical Doctors
	• Osteopathic Physicians
	• Registered Nurses
	• Clinical Units (that receive PHI)
	• Information Resources
	• Optometrists
	• Dentists
	• Dental Assistants
	• Podiatrists
	• Chiropractors
	• LPNs
	• Administrators (with rights)
	• Other Individuals and Entities
ILPD-1	Accommodate “providers” who are licensed clinicians, unlicensed clinicians, administrative personnel, organizational units, and information resources
ILPD-2	Support identity-validation and digital credentialing services for licensed clinicians, such that these providers’ entries in the ILPD will serve as official records of the providers’ digital identity
ILPD-3	Support representation of invalidated identity information provided by trusted Entities for unlicensed clinicians and non-clinician providers
ILPD-4	Support representation of invalidated identity provided by trusted Entities for licensed professionals, and automatically determine whether the information represents a new identity in the ILPD (in which case a new ILPD record is automatically created) or matches an existing identity in the ILPD (in which case the identity information is linked to the existing ILPD record)

No.	CRITICAL FUNCTIONS
ILPD-5	Support discovery of providers by their attributes, including name, provider type, location, NPI, and Entity association
ILPD-6	Support representation of and discovery of the Entities with which a discovered provider is associated, as well as the retrieval of information describing these Entities
ILPD-7	Support access to all technical information needed to exchange information with a Provider in the context of a specific Entity. This information may include the provider's unique identifier and/or digital credentials specific to that Entity, as well as information about the Node(s) through which one may communicate with the Provider at that Entity, including the transactions and interoperability protocols that those Nodes support
ILPD-8	Support read-only access via a programmatic API, which implements (at a minimum) the Messaging and Authentication Frameworks described in this document
ILPD-9	Support read-only access via a web-browser interface and limit access to only other Providers registered in the ILPD
ILPD-10	Support write access via a programmatic API, which implements (at a minimum) the Messaging and Authentication Frameworks described in this document
ILPD-11	Support write access via a web-browser which will require two-factor authentication and be logged.
ILPD-10	Store two types of information about each licensed clinician: "Discoverable" attributes that describe the clinician sufficiently to unambiguously determine her identity when accessed by other Providers and Entities and "undiscoverable" attributes that include additional information needed to credential a clinician for purposes of health plan participation, clinical privileges, etc. These two types of information must be handled separately, so that the undiscoverable attributes are only disclosed at the direction and with the consent of the Provider, whereas discoverable attributes are available to any Provider or Entity with read access to the ILPD
ILPD-11	The ILPD records of licensed clinicians must include an X.509 class-3 digital certificate signed by Cal eConnect or a certificate authority designated by Cal eConnect. The ILPD records of unlicensed clinicians and non-clinician Providers may optionally include digital certificates, which may be signed by other certificate authorities as long as there is a chain of trust to Cal eConnect or its designated certificate authority
ILPD-12	The ILPD/ELPD mapping records of licensed clinicians whose identities are certified by the Entities that submitted them must include an X-509 class-3 digital certificate signed by the Entity
ILPD-13	Support distribution and federation of service instances to ensure acceptable performance and to allow local management within designated jurisdictions (e.g., states)
ILPD-14	Meet performance requirements

No.	CRITICAL FUNCTIONS
ILPD-15	All user-interface components shall be designed to maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.
ILPD-16	All APIs shall be designed to minimize the level of effort required on the part of California stakeholders and their H.I.T. vendors to integrate their solutions with the Cal eConnect infrastructure

III.B.2.c Services Registry

Description: The Services Registry is a repository of standard interoperability protocols supported by Entities participating in the Cal eConnect Infrastructure. Cal eConnect will specify a set of such protocols for the most important and most common transactions to be conducted via the infrastructure. In the Service Registry, each Node that is registered in the ELPD will indicate standard protocols supported.3.2.1 Through this mechanism, participants in the Cal eConnect Infrastructure will be able to determine the interoperability protocols needed to exchange health information with Providers using specific Nodes in the ELPD. For further information see Exhibit B.

No.	CRITICAL FUNCTIONS
SR-1	Each interoperability protocol represented in the Services Registry must include a machine-readable description of the protocol's specifications at each level of the OSI stack, including transport method, security mechanism, message format, and vocabulary constraints. This representation must be sufficiently specific to enable a software process to determine whether it can formulate and transmit a message consistent with the specified interoperability protocol
SR-2	Each interoperability protocol must be associated with a specific transaction type, and the full set of transaction types supported by the Services Registry must be defined within it
SR-3	Provide read and write access via an WS API that is available to the ELPD only
SR-4	Provide read-only access via web browser, with no access restrictions
SR-5	Be sufficiently secure to prevent unauthorized modification or corruption of its contents via internet-based attacks
SR-6	Meet the performance requirements as specified by Cal eConnect
SR-7	All user-interface components shall be designed to maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.

No.	CRITICAL FUNCTIONS
SR-8	All application programming interfaces shall be designed to minimize the level of effort required on the part of California stakeholders and their H.I.T. vendors to integrate their solutions with the Cal eConnect infrastructure, consistent with the functional and technical requirements of these APIs

III.B.2.d Support for Complex Relationships between ILPD, ELPD, and SR

Description: Support for complex relationships that exist between Individual Providers, Provider Entities, Nodes, and Services are critical to the successful implementation and operation of the Provider Directory Services. These relationships ensure that the Provider Directories accurately reflect and support the functional and legal affiliations that are present in the healthcare system. They provide the ability for solutions that utilize the Provider Directory Services to unambiguously discover individuals, their affiliation with legal entitles, and the exact nature of the system utilized by these entities to send and receive healthcare information. They also provide the exact services supported, including the messaging frameworks, security artifacts, and payloads necessary to for two Nodes to securely communicate with each other. For further information please see Exhibit B.

No.	CRITICAL FUNCTIONS
RE-1	Each entry in the ILPD for a licensed provider may have a declared relationship with one or more entries in the ELPD. These relationships must support demographic and authorization artifacts unique to the specific relationship
RE-2	Entries in the ELPD may be hierarchical and provide for the inheritance of Node relationships created with entries higher in the hierarchy
RE-3	Each Entity may declare its own Nodes or designate the Nodes of another Entity (e.g. an HIE or HISP) as used by the Entity for a defined set of SR transactions
RE-4	If an Entity utilizes another Entities Nodes (3rd party Node), the system must allow the Entity to specify which declared services for the 3rd party Node are valid for the relationship
RE-5	Only one Node for an Entity may support a complete SR standard transaction (messaging framework, protocol, implementation guide, payload and clinical vocabulary definition)
RE-6	A Node may inherit the X.509 class-3 digital certificate from the related Entity or have its own declared certificate
RE-7	Each Node may declare that it supports one or more SR standard transactions (separately for sending and receiving) and where necessary have specific information associated with the relationship (e.g. certificate for Direct messaging protocol)

No.	CRITICAL FUNCTIONS
RE-8	A relationship between a Node and a SR standard transaction must provide for the ability to declare the use of an Exchange Service to translate the payload prior to sending / consuming or as a proxy agent for the communication with or from another Node

III.B.3 Critical Infrastructure Services: Messaging Framework; Authorization Framework; CeC Entity & Node Service and Exchange Services

III.B.3.a Messaging Framework

Description: Because the ELPD, ILPD, Services Registry and Exchange Service, as well as future services, will be developed and implemented using Web services technology, the use of messaging for service communication is a natural requirement. In order to leverage the many WS-*extensions currently available and those under development, SOAP has been chosen as the standard message format and HTTP/S as the transport protocol. Senders and receivers of HIE transactions will use the Messaging Framework when transmitting or requesting health information. The messaging framework will facilitate two core functions:

1. Provide communication between client applications and the ILPD and ELPD via a programmatic (web services) API. For example, an EHR may access the ILPD to identify Providers who are listed when initiating an exchange of health information, as well as the ability to access the ELPD for correct addressing and formatting of messages sent to those Providers.

2. Provide a communication path to the ILPD and ELPD for securely sending and receiving health information when Providers lack other means to do so.

For further information see Exhibit B.

Standards specified by WS-I Basic Profile 2.0 and WS-I Security Profile 1.1

Specification	Version	Comments
SOAP	1.2	
SOAP Message Encoding Style = Document Literal		
XML Schema	1.0	
WSDL	1.1	
HTTP	1.1	
Transport Layer Security (TLS)	1.0	
Advanced Encryption Standard (AES) with 128-bit key length		Symmetric encryption algorithm
Secure Hash Algorithm 1 (SHA-1)		Verification of message integrity in TLS
X.509 Token Profile	1.0	Digital certificates for nodes communicating via TLS

No.	CRITICAL FUNCTIONS
MF-1	SOAP messages transmitted over HTTP with Transport Layer Security (TLS). The framework will conform to the WS-I Basic Profile 2.0[1] and the WS-I Security Profile 1.1[2]. These profiles use the web-services standards specified in the above table, but prescribe further constraints to improve interoperability
MF-2	Support the following transactions and message exchange pattern (MEP)s: • Push: Deliver Laboratory Test Result to Ordering Provider and Copied Provider(s) and/or Send Ambulatory Patient Summary from One Provider to Another • Request/reply ("pull"): Request and receive information from the ELPD and ILPD and request and receive an Ambulatory Patient Summary • Publish-Subscribe: Register subscriber interest with publisher of clinical data on a specific patient. Publisher will send updates ("push") as they are available without further action on the part of the subscriber
MF-3	Use security protocols equally robust to those listed in the table above
MF-4	Have the ability to sign message contents to ensure non-repudiation of source
MF-5	Include the option to encrypt message contents for viewing by intended recipient only
MF-6	Include sufficient information and security features to allow intermediate nodes to route message contents to the final intended recipient without compromising security

III.B.3.b Authorization Framework

Description: The Authorization Framework is a set of specifications that define a trust model for exchanging health information using the messaging framework. It also describes a security model for interaction with the ILPD and ELPD via Web services. Further, this framework is intended to assure both the sender and receiver of health information that their data trading partners are who they claim to be. To anchor the trust model, a trusted Certificate Authority (Cal eConnect or an authorized third party) will certify all healthcare entities authorized to initiate and receive transactions via the Cal eConnect Infrastructure. The certification process confirms that the entities legitimately exist and follow adequate practices for securing their technical resources and user accounts.

The principle of local autonomy: The trust model ensures that providers are provisioned and authenticated by their entities at the origin of transactions. The Cal eConnect infrastructure includes no services for provider authentication, only the facility to communicate authentication

[1] See http://www.ws-i.org/Profiles/BasicProfile-2_0(WGD).html for detailed technical specifications.

[2] See http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html for detailed technical specifications.

and attribute information about providers once they have been authenticated. Similarly, all authorization decisions regarding disclosure of protected health information are made by the holders of the information, rather than within or by the Cal eConnect Infrastructure. The infrastructure includes no services to centrally manage access control rules or patient consent, etc. It contains only the facility to communicate information about Entities and Providers that are sending or requesting patient-specific health information. It is the responsibility of the Provider or Entity who holds the patient data to make authorization decisions based on this information. For further information see Exhibit B.

No.	CRITICAL FUNCTIONS
AF-1	Identity management of Entities and licensed Providers should be based on X.509 class-3 digital certificates
AF-2	Requires the inclusion of the sending Entity's digital certificate and digital signature in all transmissions
AF-3	Allows the sending Entity to authenticate the sending Provider using a variety of 1-factor or 2-factor methods, as determined by the sending Entity

III.B.3.c CaleConnect Entity and Node

Description: In addition to the core services described above, Cal eConnect intends to offer an "Entity" and operate a Node that provides certain health information exchange capabilities for Providers who may not have access to these capabilities. Every licensed Provider certified by Cal eConnect will be associated with the Cal eConnect Entity by default. This association will provide the ability to use the Cal eConnect Node for certain transactions. For further information see Exhibit B.

NO.	CRITICAL FUNCTIONS
CEN-1	Support the Messaging and Authorization Frameworks
CEN-2	Support the set of transactions for the Direct transport protocol
CEN-3	Provide a Web service that can evaluate inbound test messages submitted by developers to determine compliance with the standard interoperability protocols defined by Cal eConnect, as well as generate outbound test messages for developers to determine whether their implementations can correctly process messages compliant with the standard interoperability protocols defined by Cal eConnect
CEN-4	Provide a highly secure web-browser application that can be accessed by licensed clinicians registered in the ILPD
CEN-5	Implement two-factor authentication for access to the web-browser application
CEN-6	Provide performance and response times compatible with synchronous use by Providers

NO.	CRITICAL FUNCTIONS
CEN-7	Design all user-interface components to maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.

III.B.3.d Exchange Services

Description: A set of services implemented as Web services that bridge between disparate interoperability protocols used by participants in the Cal eConnect Infrastructure. The services are intended to translate interoperability protocols (including transport specifications and message formats) and to serve as proxies in health information transactions.

It is anticipated that, during the early adoption of the Cal eConnect Infrastructure, not all participants will be able to support Cal eConnect Interoperability Protocols. For example, certain participants may only support the transport and authorization protocol of the NwHIN Direct project, whereas others may only support the transport and authorization protocol of NwHIN Exchange or the Cal eConnect Messaging and Authorization Frameworks. Further, certain participants may be confined to proprietary formats for health information payloads, whereas others will have the capability to support standard formats established by Cal eConnect. These exchange services will have the capability to dynamically translate various disparate protocols and formats in order to facilitate information exchange among participants, who otherwise, would be unable to communicate.

Message translations that must be supported by the Contractor are:

Message Translation	From Protocol	To Protocol
Patient Care Summaries	CCD	CCR
Laboratory Results	TBD	TBD

For further information see Exhibit B.

No.	CRITICAL FUNCTIONS
ES-1	Translate message formats and transport/authentication mechanisms to semantically equivalent versions
ES-2	When acting as a proxy, must fully conform to the interoperability protocols of the sending and receiving Entities, so that these entities may generate and process the information (respectively) as if it had been sent directly from the source to the target
ES-3	When acting as a proxy, must pass through all required information and artifacts needed by the recipient to validate the sender and make authorization decisions (although the proxy may validate the sender on behalf of the recipient if it formally attests to the validation)
ES-4	When acting as a proxy, must appropriately translate and deliver any acknowledgements or other data returned from the recipient to the sender

No.	CRITICAL FUNCTIONS
ES-5	All application programming interfaces shall be designed to minimize the level of effort required on the part of California stakeholders and their H.I.T. vendors to integrate their solutions with the Cal eConnect infrastructure, consistent with the functional and technical requirements of these APIs

III.B.3.e Test Framework

Description: The Test Framework supports the development and ongoing testing of a Node's ability to support the Messaging Frameworks, APIs and full transaction definitions in the SR. It allows a vendor or Entity that owns a Node to verify that it can accurately interact with the Provider Directory and support the services defined in the SR. The Test Framework provides emulation for each of the following: a) the Provider Directory Services APIs, b) the recipient of an SR compliant transaction and c) the originator of an SR compliant transaction.

No.	CRITICAL FUNCTIONS
TF-1	Provide a web based service for a Node to test its ability to correctly utilize the messaging framework and each of the API (methods) available to the Node from the Provider Directory Services
TF-2	Provide a web based service for a Node to test its ability to formulate and send an SR compliant message in any of the messaging frameworks (Cal eConnect, Direct Project and NwHIN Exchange) and provide feedback to the testing node on inconsistent message structure where possible
TF-3	Provide a web based service for a Node to test its ability to formulate and send an SR compliant payload (e.g. CCD C32, or HL7 2.5.1 ELINCS, LOINC) and provide feedback to the testing node on inconsistent payload structure where possible
TF-4	Provide a web based service that emulates a sending Node to allow a receiving node to test its ability to receive and consume SR compliant payloads (e.g. CCD C32, or HL7 2.5.1 ELINCS, LOINC)

III.B.4 Estimated Number of Users and Client Applications

The Provider Directory Service with Exchange Capabilities should ultimately be able to support the following estimated number of California users: (See the “Performance Requirements” sections of the Functional Requirements and Technical Specifications for details):

- 700,000 entries in Individual Level Provider Directory (users)
    - 100,000 unique physicians with an average of 3 entries per unique physician
    - 200,000 unique nursing and other licensed health care providers with an average of 1 entry per unique provider
    - 200,000 unique endpoints (departments, administrators, etc) with an average of 1 entry per unique endpoint
- 60,000 entries in Entity Level Provider Directory (entities that may make requests for their associated "provider" users)
- 120,000 client applications

Others (TBD) – While the contract resulting from this RFP will be between Cal eConnect and the Contractor to benefit data trading partners in California, Cal eConnect is also in discussions with several other states to develop Memorandums of Understanding which would allow them the option to leverage Cal eConnect’s Infrastructure once implemented. The solution should support a federated architecture that allows scalability and interoperability across multiple distinct jurisdictions.

III.B.5 Environments

During the development and implementation of the Cal eConnect Infrastructure, the number of environments and their use is at the discretion of the Contractor. However, by Phase III, Development, Testing, Staging and Production environments should be in place, and at minimum, production should be separate from other environments. Post implementation, the Contractor will be responsible for maintaining technology environments as follows:

- Production environment
- Test Harness environment, to be used by Entities to test their connectivity to the infrastructure prior to transacting with the production environment
- Development and testing environment, to be used by the Contractor to implement enhancements and corrections to the infrastructure before releasing them to the staging environment
- Staging/preproduction environment, to be used by the Contractor for pre-production user acceptance testing of enhancements and corrections before releasing them to the production environment

III.C. Contractor Responsibilities

The Contractor will be responsible for performing the following tasks related to the management of the contract.

III.C.1 Contract Management

The Contractor shall provide the technical and functional activities necessary for the management of this scope of work (SOW) and activities under a resulting contract. The Contractor shall prepare, maintain, and follow a Project and Management Plan describing the technical approach, organizational resources and management controls to be employed to meet cost, schedule and performance requirements throughout contract execution. Additionally, the Contractor shall participate in project management meetings and provide weekly verbal status updates and monthly status reports monitoring the performance and progress of the contract and tasking.

III.C.1.a Task 1. Project and Management Plan

The Contractor shall prepare a Project and Management Plan outlining management approaches, automated tools to be used, key activities to be performed, and deliverable dates for products required by this SOW. This plan shall be delivered in draft no later than two weeks following Contract award.

Deliverable: Project and Management Plan

III.C.1.b Task 2. Contract Budget Tracking Report

The Contractor shall develop, maintain, and use a Contract Budget tracking process as prescribed by Cal eConnect's Project Management Office (PMO). Weekly, monthly, and on demand budget status reports are required. This process and associated reports shall be delivered no later than 30 days after award of the contract or as approved by Cal eConnect.

Deliverable: Contract Budget Tracking Report

III.C.1.c Task 3. Weekly Project Status and Progress Review

The Contractor shall participate in weekly PMO meetings and be prepared to present and discuss the following:

- Activities planned for the week
- Work and deliverables completed during the previous week
- Status of ongoing activities
- Activities planned for the following week
- Problems or issues projected or identified
- Alternatives and/or recommended solution(s) for identified or projected problems or issues, and
- Known or projected resource (staff and funding) and schedule impacts

Deliverable: Weekly Project Status and Progress Review

III.C.1.d Task 4. Monthly Project Status and Progress Summary Report

The Contractor shall prepare a monthly Project Status and Progress Summary Report, including a financial management report, and forward it in draft to Cal eConnect PMO by the 15th day of the month following the reporting period.

The report may be delivered in conjunction with the presentation of the contractor's weekly Project Status Review. The report delivered shall include weekly management issues and meetings and provide sufficient detail to ensure understanding of task progress and issues.

The final deliverable must be suitable for forwarding to Cal eConnect executive management. The format will be provided by Cal eConnect's PMO and content will include, but not be limited to, the following:

- Activities planned for the reporting period
- Work and deliverables completed during reporting period
- Status of ongoing activities
- Activities planned for the following month
- Problems or issues projected or identified
- Alternatives and/or recommended solution(s) for identified or projected problems or issues
- Known or projected resource (staff and funding) and schedule impacts
- Status of project funds including monthly and total expenditures and funds remaining

Deliverable: Monthly Project Status and Progress Summary Report

Deliverable: Monthly Financial Management Status Report

III.C.2 Quality Assurance

The Contractor shall implement a Quality Assurance (QA) process as defined by Cal eConnect's PMO control management framework. The QA process is focused on monitoring and evaluating specific metrics that measure progress and efficiency in the performance of contractual tasks. The process is performance and incentive based. Areas to be monitored include quality of deliverables; adherence to target dates and overall schedule; technical effectiveness and performance of the provider directory services; cost and; risk management.

The Bidder must describe QA methodology used in previous projects which include performance metrics and processes, as well as methods used for calculating and receiving incentives. The way in which incentives are measured and awarded will be determined during the contract negotiation process with the awarded Contractor. These metrics shall be incorporated in the periodic progress, financial, and Contract management reports that are to be submitted under this Contract.

III.C.2.a Task 5. Performance Based Services Plan

In collaboration with Cal eConnect's PMO, the Contractor shall draft a Performance Based Services Plan (PBSP) that conforms to the PMO criteria and negotiated performance incentives. Performance measures include, but are not limited to:

- Quality of deliverables and products
- Schedule Performance

- Technical Efficiency and Performance
- Working Relationships
- Cost Performance
- Risk Management

Deliverable: Performance Based Services Plan

III.C.2.b Task 6. Performance Based Services

The PBSP may be revised by mutual agreement as the operational and/or program priorities change. Either the Contractor or Cal eConnect may suggest changes in writing at any time.

Cal eConnect will retain a fixed five-percent of the Contractor's monthly labor billings in an incentive award pool. On a quarterly (three-month) basis, using the criteria and formulas described in the finalized PBSC Plan, Cal eConnect will calculate an incentive award amount based on the balance of the incentive award pool, and (via a determination letter), authorize the Contractor to bill the awarded amount in the invoice for the month that follows the evaluated period.

The Contractor shall report the status of unallocated incentive funds and the monthly five-percent labor billings being withheld in the monthly financial status report submitted each month.

Since it is Cal eConnect's intended purpose to work closely with the Contractor to obtain exceptional and cost effective services, the Cal eConnect PMO will communicate all concerns, issues, problems, and risks to the Contractor to ensure maximum ability of the Contractor to avoid loss of any withheld funds and be rewarded the maximum amount each quarter. Cal eConnect, through its PMO, will monitor the Contractor's performanceAt the end of each quarter-annual (three month) time period, Cal eConnect's PMO will prepare a written report summarizing the overall results of the Contractor's performance during the previous three-month period.A performance award will be considered and may be made on a quarterly basis to coincide with the Performance Reporting process. Within thirty (30) calendar days after receipt of the PMO's written performance summary, Cal eConnect shall notify the Contractor by letter the determination of a performance award.

The Contractor will not be entitled to re-perform, perform late, or otherwise correct defective services to improve an existing performance rating for the purposes of receiving a full performance award that would otherwise have been warrantable. At the sole discretion of Cal eConnect and upon the notification to the Contractor, the Contractor may be required to re-perform or perform late defective work disclosed by Cal eConnect inspection including defective and incomplete performance. Cal eConnect will notify the Contractor promptly if re-performance is required.

Exception If Contractor Is Not at Fault

The Contractor shall not be liable for loss of withheld funds when delays or failures arise from causes beyond the control of and without the fault or negligence of the Contractor. Such causes may include, but or not limited to: Acts of God or of the public enemy, acts of the Government in either its sovereign or contractual capacity, fires, floods, epidemics, quarantine restrictions, strikes, freight embargoes and unusually severe weather; but in every case the delay must be completely beyond the control of and without the fault or negligence of the Contractor. If the delays or failures are caused by the default or other action of a subcontractor, the Contractor shall be liable for loss of withheld funds unless the default arises out of causes completely beyond the control of both the Contractor and subcontractor and completely without the fault or negligence of either party.

III.C.2.c Task 7. Quality Assurance Surveillance Plan

The Cal eConnect PMO will review, for completeness, all preliminary or draft products that the Contractor submits, and may return them to the Contractor for correction. The Cal eConnect PMO will review, for acceptance, all final written deliverables and technical products that the Contractor submits using the general and deliverable specific criteria contained in the Exhibit C Quality Assurance Surveillance Plan (QSAP) and may return them to the Contractor for correction if necessary to meet acceptable quality standards.

The absence of comments by the Cal eConnect PMO will not relieve the Contractor of the responsibility for complying with the requirements of this work statement. Final approval and acceptance of products required herein shall be by letter of approval and acceptance by the PMO. The Contractor shall not construe any letter of acknowledgment of receipt of products as a waiver of review, or as an acknowledgment that a product is in conformance with this work statement. Any approval given during preparation of a product, or approval for shipment shall not guarantee the final acceptance of the completed product. Evaluation and acceptance of deliverables shall be conducted as outlined in the attached Quality Assurance Surveillance Plan.

III.C.3 Compliance with Cal eConnect Policies and Procedures

Bidders should become familiar with Cal eConnect's policies and procedures related to conflict of interest, procurement, and transparency.

- Conflict of Interest Policy (http://www.caleconnect.org/content/2010/11/04a.Approved-Conflict-of-Interest-Policy_11910-2-FINAL-copy.pdf)
- Procurement Policy (http://www.caleconnect.org/content/2010/05/Approved_Procurement_Policy__111110_Final.pdf)
- Transparency Policy (http://www.caleconnect.org/content/2010/11/04b.Approved-Transparency-Policy_111110-Final-copy.pdf)

III.C.4 Electronic Library

Contractor will provide and maintain an electronic library of project documentation accessible to Cal eConnect's PMO and will include, but not be limited to:

- Project deliverables, both draft and approved versions
- Project status reports
- Project work plan and assignments
- Project staff contact information
- Relevant emails, memos, and other documents that provide a comprehensive history of the Provider Directory Services with eHIE Capabilities project
- Must be accessible to Cal eConnect, CHHS, and ONC upon request

III.C.5 End-of-Contract Transition

In the event of a change in contractors at the end of the contract period, Cal eConnect will conduct a full transition from the Contractor to the successor contractor. End-of-contract transition activities to be conducted by the Contractor include, but are not limited to:

1) Participation in transition work plan development
2) Assisting in provider conversion, as needed
3) Equipment transfer of Cal eConnect-owned equipment
4) Equipment change-out for Contractor-owned equipment
5) Data cleansing of Cal eConnect Infrastructure system data
6) Data conversion requirements definition and testing of files and data records to be transferred from the Contractor to the successor contractor
7) Call center transition planning
8) Cal eConnect Infrastructure conversion planning, testing, rehearsals, and execution
9) System and process documentation
10) System interface contracts and source code related to the interfaces
11) Knowledge transfer

To prepare for end-of-contract transition, the Contractor will be required to develop and maintain a System Transition Plan. The plan will need to describe all activities to successfully transition to the new system, sequencing of those activities, the parties responsible for performing activities, and a backup plan, if any or all of the transition activities are delayed.

Cal eConnect would execute a work authorization for the Contractor to execute end-of-contract transition services.

Deliverable: System Transition Plan

III.D. Phasing of Deliverables

The phasing of deliverables is focused on a gradual rollout of the Cal eConnect Infrastructure. The primary expansion of deliverables is focused on the methods of maintenance and interaction with the ILPD and ELPD. The Exchange Services will be deployed gradually based on specific EMR vendor and transaction volumes and critical needs.

	Phase 1	Phase 2	Phase 3
Date	Q1 2012	Q2 2012	Q3 2012
HIE-to-HIE (HIEs)	2 – 4 nodes	5 – 10	11 – 20
NwHIN Direct (ELPD nodes)	2 – 4 nodes (trials)	8 – 12	20 – 50
Providers (ILPD entries)	< 100 entries	100 – 150	300 – 500
EHR-to-EHR where the EHR's use the same Protocol (entities)	2 – 4	20 – 50	500 – 1500
EHR-to-EHR via Exchange Service (entities)	1 – 2	5 – 10	100 – 300
Entity Level Provider Directory			
• Entities	5 – 10	500 – 2,000	6,000 – 12,000
• Percent of entity population (assuming 40,000 – 60,000 population)	< 1%	1 – 5%	10 – 20%
• Certification Method (Certification process will initially be performed manually by Cal eConnect or the Vendor. Over time automation will reduce/minimize manual intervention, but manual intervention/review will never go away.)	Manual (by Cal eConnect/ Vendor)	Semi-Automated (by Cal eConnect/ Vendor/ Individual)	Automated (by Individual)
Individual Level Provider Directory			
• Individual Licensed Providers	500 – 2,000	3,000 – 5,000	30,000 – 50,000
• Percent of Individual Licensed Providers population (assuming 500,000 population)	< 1 %	1 – 5%	10 – 15%
• Certification Method (Certification process will initially be performed manually by Cal eConnect or the Vendor. Over time automation will reduce/minimize manual intervention, but manual intervention/review will never go away.)	Manual (by Cal eConnect/ Vendor)	Semi-Automated (by Cal eConnect/ Vendor/ Individual)	Automated (by Individual)

	Phase 1	Phase 2	Phase 3
Services Registry			
- Interoperability Protocols	1 – 4	10 – 20	30 – 100
- Percent of population of protocols supported by Cal eConnect	<1%	5 – 10%	30 – 50%
Exchange Services			
- Translators	1 – 4	10 – 20	30 – 100
- Percent of population of protocol translators supported by Cal eConnect	<1%	5 – 10%	30 – 50%

IV PROPOSAL SUBMISSION REQUIREMENTS

Bidders are expected to provide Cal eConnect with as much information as necessary in their proposal for Cal eConnect to objectively evaluate the proposal and Bidder qualifications. At a minimum, proposals must be fully responsive to the specific requirements stated in this RFP. Bidders must identify any requirements of this RFP that they cannot satisfy. All responses to the RFP must comply with the requirements of this section.

All responses and all requested documents should be structured in the same order and lettering/numbering format as shown in the following subsections, submitted in a 3-ring binder, on 8 ½ x 11 paper, single-sided, and using at least 11-point font, consecutively numbered and sections clearly marked or labeled. Responses must be packaged and submitted in compliance with Section IV.G, Proposal Packaging and Delivery.

IV.A.Mandatory Submittals

Failure to submit all information listed under Section IV.A, Mandatory Submittals, may at the discretion of Cal eConnect, result in the rejection of the proposal. If all Bidders fail to meet one or more of the mandatory requirements, Cal eConnect reserves the right to continue evaluating the proposals. Bidders must complete and submit the following attachments as detailed below:

IV.A.1 Transmittal Letter

Bidder must submit a cover letter indicating that the Bidder is responding to the RFP and that all of the mandatory requirements in RFP have been met. The letter must be signed by a representative that is legally authorized to contractually bind the Bidder.

Bidder must also disclose any potential, actual or apparent conflicts of interest that may arise between any of the Bidder’s current clients and/or employees, and Cal eConnect. Because of the complexities involved in defining conflicts of interest, please identify any potential conflicts. Cal eConnect will make a final determination as to whether a disqualifying conflict exists. **Note: If there are no known conflicts, provide a statement to this effect.**

IV.A.2 Minimum Corporate Experience Summary Form (Attachment A)

Bidder must complete and submit Attachment A, Minimum Corporate Experience Summary Form, to document that it meets the minimum corporate experience in requirements.

IV.A.3 Corporate Experience Client Reference Form (Attachment B)

Bidders must use this form to document the three project references required in Section IV.B Company Background and Experience.

IV.A.4 Project Team Form (Attachment C)

Bidder must complete and submit Attachment C, Project Team Form, to document the project team members and their responsibilities.

IV.A.5 Minimum Staff Experience Form (Attachment D)

Bidder must complete and submit Attachment D, Minimum Staff Experience Form, to document that the minimum staff experience requirements have been met.

IV.A.6 Pre-Existing Software Form (Attachment E)

Bidder must complete and submit Attachment E, Pre-Existing Software Form, to itemize the Contractor, open source, or other licensed third-party pre-existing software that will be used in the Contractor's solution, including development, test, training and other support tools. Where Bidder's proposed solution utilizes licensed products that may constrain Cal eConnect Policy decisions please indicate what terms may need negotiation prior to release.

IV.B.Company Background and Experience

IV.B.1 Corporate Qualifications

It is Cal eConnect's belief that no single Bidder can accomplish the complete scope of work described in Section III of this RFP. In this section of the proposal, the Bidder should demonstrate how their Bidder consortium's experience and resources make it best suited to provide the required services and infrastructure. To demonstrate its background and experience, each Bidder is to provide a narrative (**6 page maximum**) that describes their relevant experience and the stability of the Bidder's organization.

For each subcontractor being proposed who will receive **twenty percent or more of the contract value**, provide the same information for the subcontractor and their proposed role (e.g., software, integration services, hosting services, etc.). Up to two additional pages may be added for each subcontractor. Bidder should describe their prior experience working with this vendor consortium.

While it is the Bidder's responsibility to decide what information under this general heading would be most useful to Cal eConnect in assessing the Bidder's capabilities, at a minimum the Bidder should include the following in this section:

- Narrative description of company history
- Number of years in business
- Number/locations of offices
- Gross Revenue for last 3 fiscal years
- Number of salaried employees (W-2) for last 3 fiscal years
- Number of contracted employees (1099) for last 3 fiscal years
- Ownership status (private/public corporation, subsidiary, etc.)
- List of projects/clients related to health care systems, health information exchanges, hosting, operating, and maintaining web-based systems, or other relevant projects/clients
- Formal partnerships with other companies
- Certifications/awards

Minimum Corporate Experience Requirements

The Bidder or Bidder consortium must be able to meet the following minimum corporate experience requirements:

1. Minimum of 5 years in business
2. Minimum of 6 healthcare client projects, including at least 1 with inter-enterprise exchange among diverse partners using a provider directory
3. Minimum of 3 client projects that implemented systems to exchange health information among independent organizations via the public internet and appropriate security and

access-control techniques. The systems must be or have been in production with at least 200 users or 5,000 transactions/year

4. Familiarity with HITECH, the ONC, CMS' EHR Incentive Program and the Meaningful Use Criteria, NwHIN and related standards, etc.
5. Technical and functional knowledge of HIT data representation, transport protocols, directory services, trusts frameworks, & related standards/methods
6. Experience with large-scale transaction-based systems that displays the capability to ensure flexibility and scalability
7. Experience hosting and operating a web services solution in compliance with HIPAA security controls
8. Experience providing support (including help desk and technical on-boarding) to a large number of users and organizations

Bidders must complete Attachment A, Minimum Corporate Experience Summary Form to document it has met these minimum experience requirements. For the purpose of defining a project to meet the above minimum requirements:

- Project must have been substantially completed within the past ten (10) years (as of the RFP Response Submission Date)
- Project must have been performed for a client external to the Contractor's / Subcontractor's organization, parent company, and subsidiaries
- Contractor / Subcontractor must have been the responsible party for completing the project

Desirable Corporate Experience Requirements

Cal eConnect will also consider the following desirable corporate experience in evaluating Bidders' experience:

1. Experience managing the impact of changes due to evolving federal or state policies
2. Experience with partnered development and revenue sharing agreements
3. Experience billing and collecting payments based upon a client's predetermined fee schedule, with respect to subscription fees, transaction fees, etc.

Corporate Experience Client Reference Form

Bidders must provide three (3) company project references for projects that are recent and similar in solution, size, or complexity to Cal eConnect's provider directory services with eHIE capabilities infrastructure project. At least one (1) company project reference shall be for the creation/deployment, and operation of a provider directory. To meet this requirement, the Bidder's project references must meet the following constraints:

- All referenced projects must have been substantially completed within the past ten (10) years (as of the RFP Response Submission Date).
- All referenced projects must have been performed for a client external to the Contractor's / Subcontractor's organization, parent company, and subsidiaries.
- Contractor / Subcontractor must have been the responsible party for completing the referenced project (prime contractor).

Bidders must use Attachment B, Corporate Experience Client Reference Form to provide three client references. Cal eConnect may contact the references following submission of the proposals to validate the information provided.

IV.B.2 Staff Qualifications

Cal eConnect is interested in the qualifications of the proposed team members who will be working the contract. Bidders must submit a project team organizational chart indicating reporting relationships of proposed project staff with roles that relate to the Bidders' approach and methodologies described in Section IV.C. Proposed Approach to the Scope of Work below.

In no more than **ten (10) pages**, including the organization chart, the Bidder must identify the specific individuals to be assigned to the roles identified in the Project Team Organization Chart, with additional details provided relative to their specific area of expertise and qualifications for this engagement.

For each individual identified, the Bidder shall provide an attached professional resume with three (3) references. Cal eConnect may contact the references to validate the information provided. Resumes are not included in the above ten page limit. Resumes should include the following information, as appropriate:

- Formal education and level achieved
- Work experience, with time ranges, and descriptions that show experience directly related to the project approach proposed by the Bidder
- Membership in professional associations
- Three (3) professional references

Bidders must complete and submit Attachment C, Project Team Form and Attachment D, Minimum Staff Experience Form. Higher ratings will be given for staff that exceeds the minimum personnel experience requirements.

Minimum Staff Experience Requirements

1. The Proposed Project Manager must be currently certified by the Project Management Institute as a Project Management Professional
2. Minimum of 5 years' experience designing, developing, and implementing IT solutions
3. Experience with at least 1 client project with inter-enterprise exchange among diverse partners using a provider directory
4. Experience with at least 1 client project that implemented systems to exchange health information among independent organizations via the public internet and appropriate security and access-control techniques. The systems must be or have been in production with at least 200 users or 5,000 transactions/year
5. The Contractor's Key Personnel must possess good verbal and written English communication skills

IV.C.Proposed Approach to the Scope of Work

Bidders must describe their proposed approach to designing, developing and implementing the Provider Directory Services with eHIE Capabilities for Cal eConnect, as described in Section III, Scope of Work. Written deliverables must be provided electronically in Microsoft Office 2010 file formats or Acrobat Reader 8.0.

IV.C.1 Services to be Delivered

The Services to be Delivered section is limited to **35 pages**. Detailed requirements for each subsection in Section III.A, Services to be Delivered, are below:

1. System Design, Development, and Implementation

Bidders must provide their approach for the design, development, testing, and implementation of their proposed solution, described in Section III.A.1. The project activities described in Section III.A.1 follow the traditional "waterfall" system development lifecycle. Bidders are permitted to propose other project approaches (such as "agile" development), but must meet Cal eConnect's aggressive timeframe for implementing Phase 1, while maintaining production and delivery of high quality, cost effective products.

2. Hosting and Data Center Operations

Bidders must describe their hosting services approach in a secure environment, as described in Section III.A.2. In particular Bidders should describe:

1. Their approach to providing each service listed in Section III.A.2 of the Scope of Work.
2. The specific controls in use that comply with the HIPAA security control requirements for each of the following:
   a. Physical Safeguards:
      i. Facility Access Controls
      ii. Workstation Use
      iii. Workstation Security
      iv. Device and Media Controls
   b. Administrative Procedures:
      i. Security Management Process
      ii. Assigned Security Responsibility
      iii. Workforce Security
      iv. Information Access Management
      v. Security Awareness and Training
      vi. Security Incident Procedures
      vii. Contingency Planning
      viii. Evaluation
      ix. Business Associate Contracts and Other Arrangements
   c. Technical Safeguards:
      i. Access Controls
      ii. Audit Controls
      iii. Integrity

iv. Person or Entity Authentication

v. Transmission Security

3. Their approach to meeting the hosting service performance requirements described in Exhibit C.
4. Cal eConnect may choose to host the Provider Directory Services with eHIE Capabilities solution at a separate facility not affiliated with the Contractor. Bidder should also describe its approach to providing maintenance and operations services for a solution hosted at a third-party facility. In addition, in the Bidder's Cost Proposal, the Bidder should provide the cost estimate for full services (including hosting at the Bidder's facility), and also list a deduction amount if the solution is hosted at a separate facility.

3. Data Acquisition Strategy

Bidder should describe their proposed approach to meeting the requirements described in Section III.A.3 of the Scope of Work. Bidder should describe any existing relationships with provider data sources.

4. Service Adoption and Utilization

Bidder should describe their proposed approach to meeting the requirements described in Section III.A.4 of the Scope of Work. Bidder should describe any experience performing such tasks.

5. Provider Certification and Maintenance (Verification and Validation)

Bidder should describe their proposed approach to meeting the detailed requirements described in Section III.A.5 of the Scope of Work. The Bidder should describe their approach under three separate assumptions:

- Bidder provides full services as a certificate verification organization (CVO)
- Bidder provides intermediate certification services (up to Bidder to propose)
- Bidder provides no certification services. Certification is performed by Cal eConnect or another party

In addition, in the Bidder's Cost Proposal, the Bidder should provide the cost estimate for full services (assuming the CVO assumption above), and also list a deduction amount for each of the other two options (intermediate services, and no certification services).

6. Reporting and Auditing Services

Bidder should describe their proposed approach to meeting the requirements described in Section III.A.6 of the Scope of Work.

7. Technical Assistance on Policy Operations Development

Bidder should describe their proposed approach to meeting the requirements described in Section III.A.7 of the Scope of Work.

8. Fraud Prevention and Monitoring

Bidders must provide their proposed approach to meeting the requirements described in Section III.A.8 of the Scope of Work.

9. Call Center and Data Trading Partner Support

Bidder should describe their approach to meeting the Call Center requirements described in Section III.A.9 of the Scope of Work. In addition to describing their approach to providing day-to-day Call Center support, the Bidder should also describe their approach to coordinating and supporting planned upgrades and managing increased Call Center demand.

In addition, Cal eConnect may choose to perform its own Call Center tasks, or contract with a separate third-party vendor not affiliated with the Contractor to provide these services to Cal eConnect. Bidder should describe its approach to providing—to Cal eConnect or a third-party selected by Cal eConnect— day to day Call Center support activities, and subsequent support of planning upgrades and managing increased Call Center demand. In the Bidder's Cost Proposal, the Bidder should provide the cost estimate for full services of meeting the Call Center and also list a deduction from the full amount if only day-to-day Call Center support activities are required.

10. Billing and Accounts Receivable Services

Bidder should describe their proposed approach to meeting the Billing and Accounts Receivable requirements described in Section III.A.10 of the Scope of Work.

In addition, Cal eConnect may choose to perform its own billing and accounts receivable tasks, or contract with a separate third-party vendor not affiliated with the Contractor to provide these services to Cal eConnect. Bidder should describe its approach to providing—to Cal eConnect or a third-party selected by Cal eConnect—the data necessary to perform billing activities. In addition, in the Bidder's Cost Proposal, the Bidder should provide the cost estimate for full services (including providing Billing and Accounts Receivable services), and also list a deduction from the full amount if only the data necessary to perform billing and accounts receivable activities is required.

11. Exchange Services Capability

Bidder should describe its approach to providing the exchange services to data trading partners that will facilitate early adoption of the Cal eConnect Infrastructure. The Bidder should describe its approach to supplying required Exchange Services Capability described in section III.A.11. Bidder should also describe the existing translations that its proposed solution can already provide.

Note: Description of any OPTIONAL Value-Add Exchange Services and Bidder's approach to sustainability should be included in a separate section, as described in section IV.E, Optional Value-Add Exchange Services and Approach to Sustainability.

IV.C.2 Solution to Functional and Technical Requirements

Bidders must describe their solution (**50 pages maximum**) to meeting the functional requirements described in Section III.B of the Scope of Work. Bidders should begin by providing an initial overview of their proposed solution, and then provide detailed descriptions of each functional area.

Exhibit B, Functional and Technical Criteria, is provided as a guideline for understanding, at a more detailed level where required, the functional requirements described in Section III.B of the Scope of Work. Bidders do not need to propose the same architecture or necessarily respond to the detailed functions described in this Exhibit B unless it is necessary to be compliant with the description of the Critical Functions in the Scope of Work.

In describing their proposed solution, the functionality listed in the Critical Functions tables of Section III.B **must** be met by the Bidder's proposed solution. For other functionality described in Section III.B, the Bidder is free to propose solutions that are **functionally equivalent** to the described functionality. Bidders should also complete and submit Attachment E, Pre-Existing Software Form, to document all Contractor, open source, or other licensed third-party pre-existing software that will be used in the Contractor's solution, including development, test, training and other support tools.

IV.C.3 Contractor Responsibilities

Bidders must describe their proposed approach to providing the services described in Section III.C, Contractor Responsibilities. The approach to Contractor Responsibilities is limited to **20 pages**.

1. Contract Management

Bidders must provide their proposed approach to meeting the requirements described in Section III.C.1 of the Scope of Work. Bidder's approach should describe the tasks, roles and responsibilities, and tools used to meet the contract management requirements.

2. Quality Assurance

Bidders must provide an example of Quality Assurance methodology used in previous projects in no more than **5 pages.**

3. Compliance with Cal eConnect Policies and Procedures

Bidders must provide their proposed approach to meeting the requirements described in Section III.C.3 of the Scope of Work.

4. Electronic library

Bidders must provide their proposed approach to meeting the requirements described in Section III.C.4 of the Scope of Work.

5. End-of-Contract Transition

Bidders must provide their proposed approach to meeting the requirements described in Section III.C.5 of the Scope of Work.

IV.C.4 Proposed Project Schedule

Each Bidder's Proposed Approach must include a proposed project schedule that is appropriate based on the Bidder's experience and approach. The schedule must include the tasks identified by the Bidder in response to the requirements of this Section IV.C for Phase 1, Phase 2, and Phase 3 (See Section III.D, Phasing of Deliverables for a description of the project phases). The schedule should include tasks, milestones, and task durations.

IV.D. Use Case Responses

Exhibit D includes seven use cases related to the Provider Directory Services with eHIE Capabilities infrastructure functionality and operations. Bidders are requested to answer the questions for each use case. Responses for all seven use cases should be no more than **20 pages** in total. These responses will assist Cal eConnect in further understanding the Bidder's proposed solution, as well as validate the Bidder's understanding of Cal eConnect's needs.

IV.E. Optional Value-Add Exchange Services and Approach to Sustainability

Cal eConnect believes that additional, value-added Exchange Services that leverage the Provider Directory Service infrastructure are critical to the success of developing a successful sustainability model. As such, Bidders are encouraged to propose a sustainability approach that includes both descriptions and costing of a portfolio of proposed value-added Exchange Services. Cost information for the optional services should be provided in the Bidder's cost proposal package, in compliance with section IV.F, Cost Proposal, and the instructions in Attachment F, Cost Proposal Instructions and Forms. There is no page limitation to this section.

Note: The description and cost data of any additional, value-added Exchange Services proposed is OPTIONAL will NOT be scored as part of Bidders' proposals. However, the data and sustainability approach will be considered and scored as part of the final interview for the Finalists selected for the interview process.

IV.F. Cost Proposal

Cost is a primary evaluation criterion. Evaluation in this category will be based on the lowest total estimated net cost to Cal eConnect over the two-year duration of the contract. Bidder must follow the instructions and submit the forms documented in Attachment F Cost Proposal Instructions and Forms (for both required and optional services) with its proposal. All prices given must be complete and inclusive, providing details for all ancillary costs including taxes, management, oversight, document or media copying, and travel expenses. All cost information must be separately sealed and identified as indicated in Section IV.G, Proposal Packaging and Delivery.

IV.G. Proposal Packaging and Delivery

All responses to this RFP must be received no later than **June 22, 2011, 4:00 p.m.** **Fax or electronic transmissions will not be accepted.** Mail or deliver all proposals to:

Cal eConnect
Attn: Gwyn Jackson
1900 Powell Street, Suite 1000
Emeryville, CA 94608

Response to RFP-2011-011

DO NOT OPEN IN MAILROOM

Postmark date will not constitute timely delivery. Proposals received after the above date and time **will not** be considered. Bidders are solely responsible for ensuring timely receipt of their responses.

The original proposal should be marked **"Original Copy"** and have original signatures. Any RFP attachment and/or form that requires a signature must be signed in ink (preferably in a color other than black) by a person who is authorized to bind the proposing firm. All requested documents should be submitted in a 3-ring binder, one-sided, and at least 11 point font, consecutively numbered and sections clearly marked or labeled. In addition, the proposal must be submitted on compact discs compatible with Microsoft Office 2010 or Acrobat Reader 8.0.

Responses must be submitted in a sealed package(s) addressed as above and clearly identifying the Bidder making the submission. Within the sealed package(s), the Bidder must include two separately labeled and sealed packages:

- Package #1: One original, five copies, and an electronic copy on compact disc of Bidder's response to Section IV, Proposal Submission Requirements, items IV.A, B, C, D, and E. **No cost information should be in package #1.**

- Package #2: One original, five copies, and an electronic copy on compact disc of Bidder's response to Section IV, Proposal Submission Requirements, item IV.F Cost Proposal.

V EVALUATION PROCESS

The proposal must be organized to correspond with all requirements and formats set forth in this RFP. The proposal should be clear, concise and must be complete. All information must be contained in the proposal. No assumptions will be made by Cal eConnect regarding the intentions of the Bidder in submitting the proposal. Bidders not providing all requested information may be rejected. Written proposals must be bound and organized in a manner to facilitate ease of review by evaluators.

All proposals submitted will be evaluated for form and content in accordance with the provisions stated in the final solicitation document. Clarifications may be requested from the Bidder at any phase of the evaluation process for the purpose of clarifying ambiguities in the information presented in the proposal.

V.A. Receipt of Proposals

Each proposal will be date and time marked as it is received and verified that all responses are submitted under an appropriate cover, sealed and properly identified. All proposals will remain sealed and in a secured area until opening, at which time all proposals will be opened together. **Unsealed proposals will be rejected.**

V.B. Evaluation of Proposals

V.B.1 Prequalification Evaluation

All proposals received by the time and date specified in Section II.A, Key Procurement Dates will be checked for the presence of proper identification, conformance with the proposal submittal requirements of this RFP, and the satisfaction of the minimum qualifications. Absence of required information may deem the proposal non-responsive and may be cause for rejection.

V.B.2 Proposal Evaluation

Proposals that pass the prequalification evaluation will undergo an evaluation process conducted by an Evaluation Committee composed of Cal eConnect staff and Stakeholders selected by Cal eConnect’s Chief Executive Officer or designee. These may be supported by external consultants or other designees (e.g. an extended evaluation team of subject matter experts). Corporate and staff references may be checked to validate past experience.

Bidder’s proposed approach to Section IV.E, Optional Value-Add Exchange Services and Approach to Sustainability will NOT be scored as part of the Bidder’s proposal. However, it will be considered during the Interview portion of the overall score for any Finalist candidate.

V.B.3 Cost Proposal Evaluation

The Bidder must adhere to the instructions and format set forth in Attachment F, Cost Proposal Instructions and Forms. Failure to do so may result in disqualification. Bidders must provide an overall fixed price covering all services and deliverables identified in the Section III, Scope of Work, for the duration of two years. Bidders shall also provide hourly rates by staff classification for labor costs; these hourly rates will also be used for unanticipated tasks. All prices given must be complete and inclusive, providing details for all ancillary costs including taxes, management, oversight, document or media copying, and travel expenses.

Cost proposals are initially rated proportionally as follows:

$$\frac{\textbf{Lowest Proposed Cost}}{\textbf{Bidder's Cost}} \textbf{ x Maximum Number Points = Bidder's Score}$$

The Evaluation Committee will review Bidders’ cost proposal details and assumptions for reasonableness. The Evaluation Committee may adjust the Bidder’s Cost Score if any aspect of the cost proposal appears unreasonable, including the number of hours to perform tasks, and cost assumptions. The Evaluation Committee may or may not contact the Bidder for clarification of the cost proposal prior to making this adjustment. The Evaluation Committee may also adjust the Cost Score of a Bidder invited to interview after the reasonableness of cost assumptions have been clarified in the interview.

Bidder’s cost proposal for services proposed in response to Section IV.E, Optional Value-Add Exchange Services and Approach to Sustainability will NOT be scored as part of the Bidder’s cost proposal. However, it will be considered during the Interview portion of the overall score for any Finalist candidate.

At the conclusion of the Evaluation of Proposals process, proposals will be evaluated according to the following weights:

Proposal Section	Weight
Company Background and Experience (Corporate & Staff)	20%
Proposed Solution to III.B Functional and Technical Requirements of the System	30%
Proposed Approach to III.A Services to be Delivered and III.C Contractor Responsibilities	25%
Use Case Responses	5%
Cost	20%

V.C. Interviews

Up to three (3) of the highest scoring Bidders, based on both technical and cost scores, may be selected as Finalists and be invited to interview with Cal eConnect and provide a demonstration of their solution’s capabilities. Key personnel identified in the proposal must participate in the interview. Date, time and additional details regarding the interviews will be provided to the selected Bidders.

Interview topics may include confirmation or clarification of the Bidder’s proposal. Topics may also include subjects not included as part of the Bidder’s proposal. Bidder’s proposed approach and cost proposal for Section IV.E, Optional Value-Add Exchange Services and Approach to Sustainability will be considered during the Interview process. A list of topics/questions will be provided to Finalists in advance.

At the conclusion of interviews, Bidders will be evaluated according to the following weights:

Criteria	Weight
Combined Proposal and Cost Score	50%
Interviews	50%

V.D. Best Value Evaluation

For the purposes of this RFP, the best value proposal will be the proposal that provides the best overall value to Cal eConnect and will most likely result in a contract that fulfills Cal eConnect's mandate to: 1.) award contracts to the responsible supplier submitting the best value proposal that maximizes the benefits to Cal eConnect in relation to the areas of security, competence, experience, and timely performance; 2.) take into account the particularly sensitive nature of Cal eConnect as the state governance entity responsible for expending ARRA funds as part of the ONC Cooperative Agreement; and 3.) act to promote and ensure integrity, security, honesty, and fairness in the operation and administration of Cal eConnect and its objectives.

As part of the best value proposal evaluation process, Cal eConnect may award a contract based on the proposals submitted or establish a competitive range and hold discussions with each Bidder in the competitive range. The competitive range shall be comprised of the most highly rated proposals consistent with the need for an efficient competition. If conducted, discussions will be undertaken with the intent of allowing each Bidder the opportunity to revise its proposal only in those specific areas identified by Cal eConnect during discussions. The discussions may include bargaining. Bargaining includes persuasion, alteration of assumptions and positions, give-and-take, and may apply to price, technical requirements, type of contract, or other terms of a proposed contract. Bidders may be asked to submit Best and Final Offers resulting from these discussions.

Cal eConnect may indicate to, or discuss with, each Bidder in the competitive range weaknesses, deficiencies, and other aspects of its proposal such as price, technical approach, and terms that could, in the opinion of Cal eConnect, be altered or explained to enhance materially the proposal's potential for award. The scope and extent of discussions are a matter solely within Cal eConnect's judgment.

A proposal meeting the requirements of the RFP but with the lowest Cost Proposal may not be selected if an award to a higher priced proposal, in the judgment of Cal eConnect, maximizes greater overall benefits to Cal eConnect. Cal eConnect may elect to pay a fair and reasonable rate to select a proposal that overall is superior.

VI TERMS AND CONDITIONS

The following sections document the standard terms and conditions for the contract that will result from this RFP (the “Contract” or the “Agreement”). References to exhibits and attachments in this section refer to the exhibits and attachments of the Contract, not this RFP. These terms and conditions may be modified to ensure the needs of Cal eConnect and the interest of the State and Federal government are met during the period of engagement. Any award resulting from this RFP is contingent upon the availability of funding.

A. General Terms

1. APPROVAL: This Agreement is of no force or effect until signed by both parties and approved by CHHS, if required. Contractor may not commence performance until such approval has been obtained.

2. CONTRACT TYPE:

   a. The Statement of Work defines and authorizes work on a Fixed Price basis, with a guarantee of task completion.

   b. To the extent that additional work not foreseen at the time this Contract is executed must be accomplished, Work Authorizations, as described in Section H.3 Unanticipated Tasks, will be the means for defining and authorizing such work on a Labor Hour basis.

3. Period of Performance

   a. Initial Term of Contract: The initial term of the Contract is two years.

   b. Option to Extend: Cal eConnect may unilaterally extend the term of this Contract under the same terms, conditions and prices, for services in accordance with the Statement of Work, for up to three (not to exceed five years) years from the Contract’s expiration date pursuant to any limitations in the Contract, including without limitation, Attachment 2, Cost Sheet.

4. EMERGENCY EXTENDED SERVICE: At Cal eConnect’s discretion, Contractor shall provide extended services for a period not to exceed nine months from the effective date of the Contract termination or expiration. Services shall continue to be provided by Contractor and paid for by Cal eConnect pursuant to the terms and conditions of this Contract.

5. EXTENDED SERVICE FOR CONTRACTOR CHANGE: Cal eConnect further reserves the right to continue operating under or further extend the initial Contract, or any extension thereof, on thirty (30) days notice for multiple ninety (90) day periods as Cal eConnect deems necessary for transition if a different contractor is chosen for a subsequent contract. To meet this requirement, Contractor, in consideration for entering into the Contract, shall maintain the service in a state of readiness for any such

periods after the completion of the Contract and shall fully cooperate with Cal eConnect and/or the replacement contractor. “State of readiness” means having the capability of extending the current Contract operations beyond the previously scheduled Contract term end date.

6. PROJECT MANAGEMENT AND SCOPE:

a. Overall Responsibilities of Contractor: Contractor is responsible for all tasks and Deliverables required for the design, development, operations, and maintenance of the System as described in the Statement of Work.

b. Scope: Cal eConnect initially intends to implement the Provider Directory Services with eHIE Capabilities functionality and services described in the Statement of Work. However, Cal eConnect reserves the right to add, modify, and/or delete functionality and services that are or may be supported by the System at any time on Notice to Contractor in accordance with the Work Authorization process, which may or may not incur costs that would be paid by Cal eConnect.

c. Supplemental Contracts: Cal eConnect may undertake or award supplemental contracts for work related to this Contract or any portion thereof. Contractor shall cooperate with such other contractors and Cal eConnect in all such cases. To the extent that such cooperation requires additional work on the part of Contractor which is beyond the scope of work outlined herein, the parties will follow the Work Authorization process.

d. Limitation of Authority: Only the Cal eConnect Chief Executive Officer or delegate by writing (with the delegation to be made prior to action) shall have the express, implied, or apparent authority to waive any clause or condition of this Agreement on behalf of Cal eConnect. Also, any waiver of any clause or condition of this Agreement is not effective or binding until made in writing and signed by the Cal eConnect Chief Executive Officer or delegate thereof.

7. AMENDMENT: No amendment or variation of the terms of this Agreement shall be valid unless made in writing, signed by the parties and approved as required. No oral understanding or Agreement not incorporated in the Agreement is binding on any of the parties.

8. ASSIGNMENT: This Agreement is not assignable by the Contractor, either in whole or in part, without the consent of the Cal eConnect in the form of a formal written amendment.

9. AUDIT: Contractor agrees that Cal eConnect, CHHS, and/or their designated representatives shall have the right to review and to copy any records and supporting documentation pertaining to the performance of this Agreement. Contractor agrees to maintain such records for possible

audit for a minimum of three (3) years after final payment, unless a longer period of records retention is stipulated or required by law. Contractor agrees to allow the auditor(s) access to such records during normal business hours and to allow interviews of any employees who might reasonably have information related to such records. Further, Contractor agrees to include a similar right of the State to audit records and interview staff in any subcontract related to performance of this Agreement. (Gov. Code §8546.7, Pub. Contract Code §10115 et seq., CCR Title 2, Section 1896).

10. INDEMNIFICATION: Contractor agrees to indemnify, defend and save harmless Cal eConnect and CHHS, its officers, agents and employees from any and all claims, damages and losses, including attorneys' fees, expenses, accruing or resulting to (i) any and all contractors, subcontractors, suppliers, laborers, agents and any other person, firm or corporation furnishing or supplying work, services, materials, or supplies in connection with the performance of this Agreement, and (ii) any person, firm or corporation who may be injured or damaged by the acts or omissions of Contractor (including its subcontractors, suppliers, laborers or agents) in the performance of this Agreement.

11. DELIVERABLE CURE NOTICE AND PROCESS: Cal eConnect has up to 14 calendar days following receipt of a paper-based deliverable, or 30 days for an electronic or software-based deliverable, from Contractor to either accept or reject. If rejected, Cal eConnect shall provide a Notice of Rejection explaining in writing reason(s) and/or deficiencies of deliverable. Contractor has 3 calendar days from date of Notice of Rejection to respond to Cal eConnect and up to 14 calendar days to cure any and all deficiencies. Cal eConnect reserves the right to terminate, without payment or penalty by Cal eConnect, this Agreement, in whole or in part, by notice to Contractor given not more than 15 calendar days from date of Notice of Rejection.

12. DISPUTES: Contractor shall continue with the responsibilities under this Agreement during any dispute.

13. ARBITRATION: Except as otherwise provided herein, any dispute arising out of or in connection with this Agreement will be subject to binding arbitration by a single Arbitrator with the American Arbitration Association (AAA), in accordance with its relevant industry rules, if any. The parties agree that this Agreement will be governed by and construed and interpreted in accordance with the laws of the State of California. The arbitration will be held in Alameda County. Judgment on any award rendered by the Arbitrator may be entered in any Court of competent jurisdiction. The arbitrator will not award damages or other relief inconsistent with this Agreement. Each party will be responsible for its costs of the arbitration; the cost of the arbitrator will be shared equally. Notwithstanding the parties' agreement herein to arbitrate, nothing in this Agreement will prevent either party from applying to a court of competent jurisdiction for provisional or interim measures or injunctive relief. No action by a party to seek and/or obtain injunctive relief shall be deemed a

waiver of the parties' agreement to arbitrate all claims related to this Agreement. The parties expressly further agree that any such action shall be maintained in a court of competent jurisdiction located in Alameda County, California.

14. CUMULATIVE REMEDIES: The rights and remedies of the parties set forth in this Agreement are not exclusive of, but are cumulative to, any rights or remedies now or subsequently existing at law, in equity, by statute or otherwise, except in those cases where this Agreement specifies that a particular remedy is sole or exclusive, but neither party may retain the benefit of inconsistent remedies. No single or partial exercise of any right or remedy with respect to one breach of this Agreement precludes the simultaneous or subsequent exercise of any other right or remedy with respect to the same or a different breach.

15. TERMINATION FOR CAUSE: Cal eConnect may terminate this Agreement and be relieved of the obligation to make any payments hereunder should the Contractor fail to perform the work required under this Agreement at the time and in the manner herein provided. In the event of such termination Cal eConnect may proceed with the work in any manner deemed proper by Cal eConnect or the State. All costs incurred by Cal eConnect in connection with so proceeding with the work shall be deducted from any sum due to the Contractor under this Agreement and the balance, if any, shall be paid to the Contractor following the determination of that balance.

16. TERMINATION FOR THE CONVENIENCE OF CAL ECONNECT:

a. Cal eConnect may terminate performance of work under this Contract for its convenience in whole or, from time to time, in part, if the Cal eConnect Chief Executive Officer, or designee, determines that a termination is in Cal eConnect's interest. The Cal eConnect Chief Executive Officer, or designee, shall terminate by delivering to the Contractor a Notice of Termination specifying the extent of termination and the effective date thereof.

b. After receipt of a Notice of Termination, and except as directed by Cal eConnect, the Contractor shall immediately proceed with the following obligations, as applicable, regardless of any delay in determining or adjusting any amounts due under this clause. The Contractor shall:

i. Stop work as specified in the Notice of Termination.

ii. Place no further orders or subcontracts for materials, services, or facilities, except as necessary to complete the continuing portion of the Contract.

iii. Terminate all subcontracts to the extent they relate to the work terminated.

iv. Settle all outstanding liabilities and termination settlement proposals arising from the termination of subcontracts.

c. Unless otherwise set forth in the Statement of Work, if the Contractor and Cal eConnect fail to agree on the amount to be paid because of the termination for convenience, Cal eConnect will pay the Contractor the following amounts; provided that in no event will total payments exceed fifty percent (50%) of the amount payable to the Contractor if the Contract had been fully performed:

i. The Contract price for Deliverables or services accepted by Cal eConnect and not previously paid for, adjusted for any savings on freight and other charges; and

ii. The total of: A) The reasonable costs incurred in the performance of the work terminated, including initial costs and preparatory expenses allocable thereto, but excluding any cost attributable to Deliverables or services paid or to be paid; B) The reasonable cost of settling and paying termination settlement proposals under terminated subcontracts that are properly chargeable to the terminated portion of the Contract; and C) Reasonable storage, transportation, demobilization, unamortized overhead and capital costs, and other costs reasonably incurred by the Contractor in winding down and terminating its work.

d. The Contractor will use generally accepted accounting principles, or accounting principles otherwise agreed to in writing by the parties, and sound business practices in determining all costs claimed, agreed to, or determined under this clause.

17. START WORK: Failure or refusal on the part of the Contractor to begin performance within ten (10) working days of contract execution may be treated as a repudiation of the contract at the sole discretion of Cal eConnect. For clarity, this repudiation will not be deemed a termination for convenience. Cal eConnect may then either: 1) select the next ranked proposal which conforms to the requirements of this RFP and represents, in the sole discretion of Cal eConnect, the best value proposal that maximizes the benefits to Cal eConnect; or 2) reject all proposals. Cal eConnect reserves its right to damages associated with a repudiation of the Contract.

18. INDEPENDENT CONTRACTOR: Contractor, and the subcontractors, agents and employees of Contractor, in the performance of this Agreement, shall act in an independent capacity and not as officers or employees or agents of Cal eConnect.

19. RECYCLING CERTIFICATION: The Contractor shall certify in writing under penalty of perjury, the minimum, if not exact, percentage of post-consumer material as defined in the Public Contract Code Section 12200,

in products, materials, goods, or supplies offered or sold to the State regardless of whether the product meets the requirements of Public Contract Code Section 12209. With respect to printer or duplication cartridges that comply with the requirements of Section 12156(e), the certification required by this subdivision shall specify that the cartridges so comply (Pub. Contract Code §12205).

20. NON-DISCRIMINATION CLAUSE: During the performance of this Agreement, Contractor and its subcontractors shall not unlawfully discriminate, harass, or allow harassment against any employee or applicant for employment because of sex, race, color, ancestry, religious creed, national origin, physical disability (including HIV and AIDS), mental disability, medical condition (e.g., cancer), age (over 40), marital status, sexual orientation, and denial of family care leave. Contractor and its subcontractors shall insure that the evaluation and treatment of their employees and applicants for employment are free from such discrimination and harassment. Contractor and its subcontractors shall comply with the provisions of the Fair Employment and Housing Act (Gov. Code §12990 (a-f) et seq.) and the applicable regulations promulgated thereunder (California Code of Regulations, Title 2, Section 7285 et seq.). The applicable regulations of the Fair Employment and Housing Commission implementing Government Code Section 12990 (a-f), set forth in Chapter 5 of Division 4 of Title 2 of the California Code of Regulations, are incorporated into this Agreement by reference and made a part hereof as if set forth in full. Contractor and its subcontractors shall give written notice of their obligations under this clause to labor organizations with which they have a collective bargaining or other Agreement.

21. Contractor shall include the nondiscrimination and compliance provisions of this Agreement in all subcontracts to perform work under the Agreement.

22. CERTIFICATION CLAUSES: The CONTRACTOR CERTIFICATION CLAUSES contained in the State of California document CCC 307 are hereby incorporated by reference and made a part of this Agreement by this reference as if attached hereto.

23. TIMELINESS: Time is of the essence in this Agreement.

24. COMPENSATION: The consideration to be paid Contractor, as provided herein, shall be inclusive of all of Contractor’s expenses incurred in the performance hereof, including travel, per diem, and taxes, unless otherwise expressly so provided. Except as expressly set forth in the Agreement, Cal eConnect shall have no responsibility to pay for, or to reimburse Contractor for, any of Contractor’s expenses incurred in the performance hereof. Contractor agrees to indemnify, defend and hold Cal eConnect harmless from and against any compensation and other amounts owed to any subcontractors engaged by Contractor in connection with performance under this Agreement.

25. GOVERNING LAW: This contract is governed by and shall be interpreted in accordance with the laws of the State of California.

26. ANTITRUST CLAIMS: The Contractor by signing this agreement hereby certifies that if these services or goods are obtained by means of a competitive bid, the Contractor shall comply with the requirements of the Government Codes Sections set out below.

a. The Government Code Chapter on Antitrust claims contains the following definitions:

i. “Public purchase” means a purchase by means of competitive bids of goods, services, or materials by the State or any of its political subdivisions or public agencies on whose behalf the Attorney General may bring an action pursuant to subdivision (c) of Section 16750 of the Business and Professions Code.

ii. “Public purchasing body” means the State or the subdivision or agency making a public purchase. Government Code Section 4550.

b. In submitting a bid to a public purchasing body, the bidder offers and agrees that if the bid is accepted, it will assign to the purchasing body all rights, title, and interest in and to all causes of action it may have under Section 4 of the Clayton Act (15 U.S.C. Sec. 15) or under the Cartwright Act (Chapter 2 (commencing with Section 16700) of Part 2 of Division 7 of the Business and Professions Code), arising from purchases of goods, materials, or services by the bidder for sale to the purchasing body pursuant to the bid. Such assignment shall be made and become effective at the time the purchasing body tenders final payment to the bidder. Government Code Section 4552.

c. If an awarding body or public purchasing body receives, either through judgment or settlement, a monetary recovery for a cause of action assigned under this chapter, the assignor shall be entitled to receive reimbursement for actual legal costs incurred and may, upon demand, recover from the public body any portion of the recovery, including treble damages, attributable to overcharges that were paid by the assignor but were not paid by the public body as part of the bid price, less the expenses incurred in obtaining that portion of the recovery. Government Code Section 4553.

d. Upon demand in writing by the assignor, the assignee shall, within one year from such demand, reassign the cause of action assigned under this part if the assignor has been or may have been injured by the violation of law for which the cause of action arose and (a) the assignee has not been injured thereby, or (b) the assignee declines to file a court action for the cause of action. See Government Code Section 4554.

27. CHILD SUPPORT COMPLIANCE ACT: For any Agreement in excess of $100,000, the contractor acknowledges in accordance with Public Contract Code 7110, that:

a. The Contractor recognizes the importance of child and family support obligations and shall fully comply with all applicable state and federal laws relating to child and family support enforcement, including, but not limited to, disclosure of information and compliance with earnings assignment orders, as provided in Chapter 8 (commencing with section 5200) of Part 5 of Division 9 of the Family Code; and

b. The Contractor, to the best of its knowledge is fully complying with the earnings assignment orders of all employees and is providing the names of all new employees to the New Hire Registry maintained by the California Employment Development Department.

28. UNENFORCEABLE PROVISION: In the event that any provision of this Agreement is unenforceable or held to be unenforceable, then the parties agree that all other provisions of this Agreement have force and effect and shall not be affected thereby, and the unenforceable provision shall be replaced by an enforceable provision that comes closest to the intent of the parties underlying the unenforceable provision.

29. PRIORITY HIRING CONSIDERATIONS: If this Contract includes services in excess of $200,000, the Contractor shall give priority consideration in filling vacancies in positions funded by the Contract to qualified recipients of aid under Welfare and Institutions Code Section 11200 in accordance with Pub. Contract Code §10353.

30. SMALL BUSINESS PARTICIPATION AND DVBE PARTICIPATION REPORTING REQUIREMENTS:

a. If for this Contract Contractor made a commitment to achieve small business participation, then Contractor must within 60 days of receiving final payment under this Contract (or within such other time period as may be specified elsewhere in this Contract) report to the awarding department the actual percentage of small business participation that was achieved. (Govt. Code § 14841.)

b. If for this Contract Contractor made a commitment to achieve disabled veteran business enterprise (DVBE) participation, then Contractor must within 60 days of receiving final payment under this Contract (or within such other time period as may be specified elsewhere in this Contract) certify in a report to the awarding department: (1) the total amount the prime Contractor received under the Contract; (2) the name and address of the DVBE(s) that participated in the performance of the Contract; (3) the amount each DVBE received from the prime Contractor; (4) that all payments under the Contract have been made to the DVBE; and (5) the actual percentage of DVBE participation that was achieved. A person or entity that knowingly provides false information shall be subject to a civil penalty for each violation. (Mil. & Vets. Code § 999.5(d); Govt. Code § 14841.)

31. LOSS LEADER: If this Contract involves the furnishing of equipment, materials, or supplies then the following statement is incorporated: It is unlawful for any person engaged in business within this state to sell or use any article or product as a "loss leader" as defined in Section 17030 of the Business and Professions Code. (PCC 10344(e).

32. CONFIDENTIALITY OF DATA:

a. All financial, statistical, personal, technical, strategic and other data, documents, materials and information relating to Cal eConnect's operation which are designated confidential by Cal eConnect or which by their nature may be reasonably construed to be confidential and made available to the Contractor in order to carry out this Contract, or which become available to the Contractor in carrying out this Contract ("Data" or "data"), shall be protected by the Contractor from unauthorized use and disclosure through the observance of the same or more effective procedural requirements as are applicable to Cal eConnect but no less than reasonable procedures. The identification of Cal eConnect's procedural requirements for protection of such data and information from unauthorized use and disclosure shall be provided by Cal eConnect in writing to the Contractor. If the methods and procedures employed by the Contractor for the protection of the Contractor's data and information are deemed by Cal eConnect to be adequate for the protection of Cal eConnect's confidential information, such methods and procedures may be used, with the written consent of Cal eConnect, to carry out the intent of this paragraph. The Contractor shall not be required under the provisions of this paragraph to keep confidential any data or information which is or becomes publicly available, is already rightfully in the Contractor's possession, is independently developed by the Contractor outside the scope of this Contract, or is rightfully obtained from third parties.

b. All Data is, or shall be, and shall remain the sole and exclusive property of Cal eConnect. Contractor shall cause to be executed all such assignments or other instruments or documents as Cal eConnect may reasonably request to carry out the intention of this Section. Contractor shall not prevent Cal eConnect from accessing Data during the pendency of a good faith dispute with Cal eConnect, or withhold or restrict access to Data (in whatever format) for any reason and under any circumstances.

c. Absent Cal eConnect's prior written consent (which may be withheld in Cal eConnect's sole discretion) or as otherwise directed by Cal eConnect or as required for the performance of the services under the Agreement, Data shall not be (a) used, disclosed, monitored, analyzed, individualized, anonymized, aggregated, stored, copied or otherwise provided to third parties by Contractor or its employees, subcontractors or agents, or (b) sold, assigned, or leased by Contractor or its employees, subcontractors or agents, or (c) commercially exploited in any form (including any individualized, anonymized or aggregated form) by or on behalf of Contractor or its employees, subcontractors or agents. Contractor shall at all times comply with all Cal eConnect's data retention, use and privacy standards and all laws applicable to Contractor relating to Contractor's access to Data.

d. In the event of any actual or threatened breach of the security of Data, Contractor will fully cooperate with Cal eConnect to secure Data. If any breach of security of Data is the result of any action or failure to act on the part of Contractor or one of Contractor's employees, subcontractors or agents, Contractor agrees to notify Cal eConnect immediately upon becoming aware of such breach, and if the personal or confidential data of Cal eConnect or a Cal eConnect customer, subcontractor, employee or agent is compromised or disclosed, to reimburse Cal eConnect for the cost of notification of all affected parties as well as reimbursement of any remedy to correct and mitigate the effect of any such security breach, including at least one year of credit monitoring services to any affected party whose personal or confidential data may have been compromised.

e. Contractor will not transfer any Data across a country border or to an offshore location.

33. CONTRACT COMPLETION CRITERIA: This contract will be considered complete when the Cal eConnect Project Manager has approved and accepted all assigned deliverables.

34. CONFLICTS BETWEEN DOCUMENTS; ORDER OF PRECEDENCE: In the event that there is a conflict between the documents comprising this Contract, the order of precedence shall be as follows:

a. The terms and conditions in the body of this Contract;

b. The Exhibits and Attachments to this Contract;

c. The Deliverables;

d. The RFP;

e. Contractor's Final Proposal in response to RFP-2011-011

35. WARRANTY

a. Unless otherwise specified in the Statement of Work or as otherwise mutually agreed by the parties, the warranties in this subsection a) begin upon delivery of the goods or services in question and end one (1) year thereafter. Contractor warrants that (i) Deliverables and services furnished hereunder will substantially conform to the requirements of this Contract (including without limitation all descriptions, specifications, drawings and services identified in the Statement of Work), and (ii) the Deliverables will be free from defects in materials and workmanship. Where the parties have agreed to design specifications (such as a Detailed Technical Design Document) and incorporated the same or equivalent in the Statement of Work directly or by reference, Contractor will warrant that its Deliverables provide all functionality required thereby. In addition to the other warranties set forth herein, where the Contract calls for delivery of Commercial Software, Contractor warrants that such Software will perform in accordance with its license and accompanying Documentation. Cal eConnect's approval of designs or specifications furnished by Contractor shall not relieve the Contractor of its obligations under this warranty.

b. Contractor warrants that Deliverables furnished hereunder will be free of harmful code (i.e. computer viruses, worms, trap doors, time bombs, disabling code, or any similar malicious mechanism designed to interfere with the intended operation of, or cause damage to, computers, data, or Software) Without limiting the generality of the foregoing, if Cal eConnect believes that harmful code may be present in any Commercial Software delivered hereunder, Contractor will, upon Cal eConnect's request, provide a master copy of the Software for comparison and correction.

c. Contractor hereby represents and warrants that execution, performance and delivery of this Agreement by Contractor will not conflict with or violate or result in any breach of, or constitute a default under, any contract, agreement or other obligation of Contractor.

d. Contractor shall maintain the currency of the technology and ensure that the Agreement and service levels can grow and align with Cal eConnect's clinical and business needs. All products and deliverables provided under the Agreement shall be, at Cal eConnect's option, the then-most current generally available version, release or model and will include all of the updates and upgrades that Contractor makes generally available. If any updates or upgrades require additional adaptations or adjustments to customized engineering modifications made by Contractor, Contractor shall perform such services at no additional charge.

e. Contractor represents and warrants to Cal eConnect that: (1) all products and deliverables are original works of Contractor (or are duly licensed by Contractor for the purposes for which they are delivered); (2) Contractor is the lawful owner or licensee of all materials used in connection with the development of the products and deliverables and has the rights to use and allow Cal eConnect to use such products and deliverables; (3) the use of the products and deliverables does not and will not infringe the intellectual property rights of any third party.

f. Contractor shall pass through all assignable warranties and indemnifications from any third party and will take all action as requested by Cal eConnect to enforce all pass-through rights and remedies on Cal eConnect's behalf.

g. Contractor represents, warrants and covenants that all products and deliverables shall operate together as a system and are compatible with the IT environment of Cal eConnect.

h. Contractor represents and warrants that it shall take all measures to ensure the security of the products and deliverables and all Cal eConnect data contained therein from intrusion.

i. All warranties, including special warranties specified elsewhere herein, shall inure to the benefit of Cal eConnect, the State, its successors, assigns, customer agencies, and governmental users of the Deliverables and/or services.

j. Except as may be specifically provided in the Statement of Work or elsewhere in this Contract, for any breach of the warranties provided in this Section, Cal eConnect's remedy and Contractor's obligation will be: (i) re-performance, repair, or replacement of the nonconforming Deliverable (including without limitation an infringing Deliverable) or service; or (ii) should Cal eConnect in its sole discretion consent, refund of all amounts paid by Cal eConnect for the nonconforming Deliverable or service and payment to Cal eConnect of any additional amounts necessary to equal Cal eConnect's Cost to Cover. “Cost to Cover” means the cost, properly mitigated, of procuring Deliverables or services of equivalent capability, function, and performance.

k. EXCEPT FOR THE EXPRESS WARRANTIES SPECIFIED IN THIS CONTRACT, CONTRACTOR MAKES NO WARRANTIES EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

36. ADDITIONAL WARRANTIES.

a. Four-Digit Date Compliance: Contractor warrants that it will provide only Four-Digit Date Compliant (as defined below) Equipment, Deliverables and/or Services to Cal eConnect. “Four Digit Date Compliant” Equipment, Deliverables and Services can accurately process, calculate, compare, and sequence date data, including without limitation date data arising out of or relating to leap years and changes in centuries. This warranty and representation is subject to the warranty terms and conditions of this Contract and does not limit the generality of warranty obligations set forth elsewhere herein.

b. Covenant Against Gratuities: Contractor warrants, by signing this Contract, that no gratuities (in the form of entertainment, gifts, or otherwise) were offered or given by Contractor, or any agent or representative of the Contractor, to any officer, agent, representative, or employee of Cal eConnect with a view toward securing this Contract or securing favorable treatment with respect to any determinations concerning the performance of this Contract. For breach or violation of this warranty, Cal eConnect shall have the right to terminate the Contract, either in whole or in part, and any loss or damage sustained by Cal eConnect in procuring on the open market any Equipment or Services which Contractor agreed to supply shall be borne and paid for by the Contractor. The rights and remedies of Cal eConnect provided in this clause shall not be exclusive and are in addition to any other rights and remedies provided by law or in equity.

c. Good Standing: Contractor warrants it is currently in good standing with the State Office of the Secretary of State and qualified to do business in California.

d. Power and Authority: The Contractor warrants that it has full power and authority to grant the rights herein granted and will hold Cal eConnect harmless from and against any loss, cost, liability, and expense (including reasonable attorney fees) arising out of any breach of this warranty. Further, Contractor avers that it will not enter into any arrangement with any third party which might abridge any rights of Cal eConnect under this Contract.

37. ADDITIONAL RIGHTS AND REMEDIES:

a. Withholding Payments: Cal eConnect shall have the right to withhold or delay payments to Contractor, in whole or in part, if Contractor fails to perform its obligations set forth in this Contract.

b. Release of Payment Withholds: For each month that a payment or a portion thereof is withheld, Cal eConnect shall continue to withhold said amount until Acceptance of the Deliverable or Service for which the payment withhold is associated.

38. Cover: If, in the reasonable judgment of Cal eConnect, a default by Contractor is not so substantial as to require termination, reasonable efforts to induce Contractor to cure the default are unavailing, and the default is capable of being cured by Cal eConnect or by another resource without unduly interfering with continued performance by Contractor, Cal eConnect may provide or procure the Services reasonably necessary to cure the default, in which event Contractor shall reimburse Cal eConnect for the reasonable cost of the services.

39. Right to Inspect: The Deliverables and Services being provided by Contractor and its Subcontractors, if any, pursuant to this Contract shall be available for inspection and review at any reasonable time by representatives of Cal eConnect including, but not limited to, Cal eConnect's Independent Verification and Validation vendor.

40. STOP WORK

a. Cal eConnect may, at any time, by written Stop Work Order to the Contractor, require the Contractor to stop all, or any part, of the work called for by this Contract for a period up to 90 days after the Stop Work Order is delivered to the Contractor, and for any further period to which the parties may agree. The Stop Work Order shall be specifically identified as such and shall indicate it is issued under this clause. Upon receipt of the Stop Work Order, the Contractor shall immediately comply with its terms and take all reasonable steps to minimize the incurrence of costs allocable to the work covered by the Stop Work Order during the period of work stoppage. Within a period of 90 days after a Stop Work Order is delivered to the Contractor, or within any extension of that period to which the parties shall have agreed, Cal eConnect shall either:

i. Cancel the Stop Work Order; or

ii. Terminate the work covered by the Stop Work Order as provided for in the termination for cause or the termination for convenience clause of this Contract.

b. If a Stop Work Order issued under this clause is canceled or the period of the Stop Work Order or any extension thereof expires, the Contractor shall resume work. Cal eConnect shall make an equitable adjustment in the delivery schedule, the Contract price, or both, and the Contract shall be modified, in writing, accordingly, if:

i. The Stop Work Order results in an increase in the time required for, or in the Contractor's cost properly allocable to the performance of any part of this Contract; and

ii. The Contractor asserts its right to an equitable adjustment within 30 days after the end of the period of work stoppage; provided, that if Cal eConnect decides the facts justify the action, Cal eConnect may receive and act upon a proposal submitted at any time before final payment under this Contract.

c. If a Stop Work Order is not canceled and the work covered by the Stop Work Order is terminated in accordance with the provision entitled Termination for the Convenience of Cal eConnect, Cal eConnect shall allow reasonable costs resulting from the Stop Work Order in arriving at the termination settlement.

d. Cal eConnect shall not be liable to the Contractor for loss of profits because of a Stop Work Order issued under this clause.

41. Unless otherwise exempted, news releases pertaining to this Contract shall not be made without prior written approval of the Cal eConnect Project Manager.

B. Incorporation of Procurement Guidelines

1. Contractor shall be responsible for all costs incurred by Contractor and/or by others acting on Contractor's behalf associated with Contractor's submission of any and all responses to any RFP or other solicitation by Cal eConnect related to this Agreement. Any materials submitted to Cal eConnect in connection with any such RFP or other solicitation shall become the property of Cal eConnect. Cal eConnect reserves the right to use any concepts or ideas contained in any such submission, response and related materials.

2. To the extent practicable and economically feasible, property, products and services provided pursuant to this Agreement shall be dimensioned in the metric system of measurement, shall conserve natural resources and protect the environment, and be energy efficient.

3. Contractor and its employees, subcontractors and agents must be properly licensed, certified and/or have valid permits for any of the property or services provided. Cal eConnect may request evidence thereof at any time and may maintain such evidence as part of the contract file.

4. The funds being utilized to procure the property, products and/or services Contractor is to provide hereunder are funds awarded to Cal eConnect as part of its Cooperative Agreement with the State of California for the ONC State HIE project funded by the American Recovery and Reinvestment Act. As a result, Contractor will fully cooperate with Cal eConnect and with the federal and state governments' access to procurement documents resulting from this RFP, including:

5. Permitting the HHS, HHS Office of Inspector General, the U.S. Comptroller General, or any of their authorized representatives ("Federal Auditors") or theCalifornia Department of General Services, the Bureau of State Audits, or their designated representative ("State Auditors") the right to review and to copy any records and supporting documentation pertaining to this Agreement or any response to any RFP or other solicitation related to this Agreement, to performance of Contractor and any subcontractor under this Agreement, and any subcontracts made thereunder.

6. Any subcontracts made pursuant to this Agreement shall include these provisions.

   a. If the California Health and Human Services Agency (CHHS) terminates its agreement with Cal eConnect before its scheduled termination date, and upon thirty days' notice to Contractor, this Agreement may be assigned to the State, including by not limited to CHHS, or a successor non-profit agency as the CHHS may specify.

7. Cal eConnect shall endeavor to pay all properly documented invoices within thirty days of receipt and Contractor's demonstration that it has satisfied all conditions precedent to its right to such payment, including without limitation the delivery and approval of any and all required deliverables.

8. Contractor and its employees, subcontractors and agents shall immediately report in writing to Cal eConnect any incidents of fraud or abuse.

9. Contractor and its employees, subcontractors and agents, and all products, services and deliverables provided hereunder, will comply with all applicable state and federal laws, rules and regulations, including but not limited to the Americans with Disabilities Act (ADA) of 1990 (42 USC 12101 et.seq) and California Government Code Sections 11135-11139.5, and all privacy, security and data protection laws, rules and regulations.

10. The parties acknowledge that certain services provided under this Agreement, as it may be amended from time to time, may result in employees or subcontractors of each party obtaining access to Protected Health Information ("PHI") as that term is defined at 45 C.F.R. § 160.103. The parties hereby acknowledge their intention to fully comply with the requirements for protecting PHI as set forth in (a) the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); (b) the American Recovery and Reinvestment Act of 2009; and (c) 45 C.F.R. Parts 160 and 164. Contractor agrees to execute, and to cause its subcontractors to execute, a Business Associate Agreement as Cal eConnect may request.

11. Contractor acknowledges and agrees that it will comply, and all of its subcontractors and agents will comply, with all policies and procedures of Cal eConnect and the State which may be provided to Contractor from time to time. Contractor agrees that Contractor and each of its employees, subcontractors and agents, will at all times comply with the administrative, technical and physical security and safety regulations and will maintain the security of all data and materials belonging to Cal eConnect and/or the State.

C. **Special Terms and Conditions**

ARTICLE I. GENERAL ASSURANCES AND STAFFING

A. Nondiscrimination

1. Contractor shall comply with all federal statutes relating to nondiscrimination, including but not limited to the Americans with Disabilities Act, referred to in Exhibit C, and the Equal Access to Federally-Funded Benefits, Programs and Activities (Title VI of the Civil Rights Act of 1964.). Contractor shall ensure compliance with Title VI of the Civil Rights Act of 1964 (42 U.S.C. Section 2000d; 45 C.F.R. Part 80), which prohibits recipients of federal financial assistance from discriminating against persons based on race, color, religion, or national origin.

B. Law, Policy and Procedure, Licenses, Certificates and Standards of Work

1. Contractor agrees to comply with all applicable local, State, and federal laws including, but not limited to, discrimination, wages and hours of employment, occupational safety; and to fire, safety, health, and sanitation regulations, directives, and/or guidelines related to this Agreement, and resolve all issues using good administrative practices and sound judgment. Contractor shall keep in effect all licenses, permits, notices, and certificates that are required by law.

2. Contractor agrees that the performance of work and services pursuant to the requirements of this Agreement shall conform to accepted professional standards.

3. This Agreement is subject to the federal Department of Health and Human Services Administrative requirements, which can be found at 45 CFR Part 74 and the Standard Terms and Conditions implemented through the HHS Grants Policy Statement located at http://www.hhs.gov/grantsnet/adminis/gpd/index.htm .

C. Fraud and Abuse

1. Contractor shall report immediately to Cal eConnect, in writing, any incidents of alleged fraud and/or abuse either by the Contractor or by any of the Contractor's employees, subcontractors or agents. Contractor shall maintain any records, documents, or other evidence of fraud and abuse until otherwise notified by Cal eConnect.

2. Contractor shall promptly refer to the HHS Office of Inspector General any credible evidence that a principal, employee, agent, contractor, sub-recipient, subcontractor, or other person has submitted a false claim under the False Claims Act or has committed a criminal or civil violation of laws pertaining to fraud, conflict of interest, bribery, gratuity, or similar misconduct involving those funds. The HHS Office of Inspector General can be reached at http://www.oig.hhs.gov/fraud/hotline/.

D. Conflict of Interest

1. The Contractor shall prevent employees, consultants, or members of governing bodies from using their positions for purposes including, but not limited to, the selection of Contractor, that are, or give the appearance of being, motivated by a desire for private gain for themselves or others, such as family, business, or other ties. The Contractor shall comply with specific requirements for Conflict of Interest, as specified by Cal eConnect. Cal eConnect reserves the right to request that the Contractor provide reports and/or analysis of required disclosure statements, and other supporting information.

2. In the event that it is determined that a conflict of interest exists, any increase in costs associated with the conflict of interest may be disallowed by Cal eConnect and such conflict may constitute grounds for termination of the Agreement for cause.

E. Covenant Against Contingent Fees

1. Contractor warrants that no person or selling agency has been employed or retained to solicit this Agreement. There has been no agreement to make commission payments in order to obtain this Agreement.

2. For breach or violation of this warranty, Cal eConnect shall have the right to void this Agreement without liability, or at its discretion to deduct from the Agreement price or consideration, or otherwise recover, the full amount of such commission, percentage, brokerage, or contingency fee.

F. Payroll Taxes and Deductions

1. Contractor shall promptly forward payroll taxes, insurances, and contributions, including State Disability Insurance, Unemployment Insurance, Old Age Survivors Disability Insurance, and federal and State Income taxes withheld, to designated governmental agencies as required by law.

G. Contractor shall comply with all applicable orders or requirements issued under the following laws:

1. Clean Air Act, as amended (42 USC 1857).

2. Clean Water Act, as amended (33 USC 1368).

3. Federal Water Pollution Control Act, as amended (33 USC 1251 et seq.).

4. Environmental Protection Agency Regulations

   a. (40 CFR, Part 15 and Presidential Executive Order 11738).

5. Public Contract Code Section 10295.3, concerning discrimination.

H. Debarment, Suspension, and Other Responsibility Matters

1. Contractor certifies to the best of its knowledge and belief, that it he/she and their principals or affiliates or any subcontractor or agent used under this agreement:

   a. Are not presently debarred, suspended, proposed for disbarment, declared ineligible, or voluntarily excluded from covered transactions by any federal department or agency;

   b. Have not within a three-year period preceding this Agreement been convicted of or had a civil judgment rendered against them for commission of fraud or a criminal offense in connection with obtaining, attempting to obtain, or performing a public (federal, State, or local) transaction or contract under a public transaction; violation of federal or State antitrust statutes or commission of embezzlement, theft, forgery, bribery, falsification or destruction of records, making false statements, or receiving stolen property;

   c. Are not presently indicted for or otherwise criminally or civilly charged by a governmental entity (federal, State, or local) with commission of any of the offenses enumerated in paragraph (1)(b) of this certification; and

   d. Have not within a three-year period preceding this Agreement had one or more public transactions (federal, State, or local) terminated for cause or default.

   e. Contractor also certifies that neither it nor any of its subcontractors or agents are listed on the Excluded Parties Listing System (http://www.epls.gov) (Executive Order 12549, 7 CFR Part 3017, 45 CFR Part 76, and 44 CFR Part 17).

2. Contractor agrees to timely execute any and all amendments to this Agreement or other required documentation relating to its, or its subcontractors' or agents', debarment or suspension status.

I. Lobbying Certification. Contractor, by signing this Agreement, hereby certifies to the best of his or her knowledge and belief, that:

1. No federally appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any federal contract, the making of any federal grant, the making of any federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any federal contract, grant, loan, or cooperative agreement.

2. If any funds other than federally appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any federal agency, a Member of Congress, an officer or employee of Congress or an employee of a Member of Congress in connection with this federal contract, grant, loan or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, "Disclosure Form to Report Lobbying," in accordance with its instructions.

3. Contractor shall require that the language of this certification above be included in the award documents for all subcontracts (including sub-grants, and contracts under grants, loans, and cooperative agreements which exceed $100,000) and that all subcontractors shall certify and disclose accordingly.

4. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. This certification is a prerequisite for making or entering into this transaction imposed by Section 1352, Title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

ARTICLE II. SUBCONTRACTS OR SUB-RECIPIENT AWARDS

A. Nothing contained in this Agreement shall create any contractual relationship between Cal eConnect and any subcontractor, supplier or agent of Contractor ("Subcontractors" or "subcontractors"), and no Subcontractor shall relieve Contractor of its responsibilities and obligations hereunder.

1. Contractor agrees to be fully responsible to Cal eConnect for the acts and omissions of its Subcontractors and of persons either directly or indirectly employed by any of them as it is for the acts and omissions of persons directly employed by Contractor.

2. Any Subcontractor used by the Contractor are accountable to Contractor and must meet the requirements of this Agreement when performing services funded by this Agreement.

3. Contractor's obligation to pay its Subcontractor is an independent obligation from the obligation of Cal eConnect to make payments to the Contractor. Cal eConnect shall have no obligation to pay or to enforce the payment of any moneys to any subcontractor.

B. Notwithstanding Section B above, Cal eConnect shall include the following provision in all subcontracts or sub-recipient awards:

1. "If the California Health and Human Services Agency (CHHS) terminates its agreement with Cal eConnect before its scheduled termination date, and upon thirty days notice to the subcontractor or sub-recipient, any contract or sub-recipient award may be assigned by the California Health and Human Services Agency (CHHS) to the State, including but not

limited to CHHS, or a successor non-profit agency as the CHHS may specify."

C. In accordance with federal procurement regulations, all procurement transactions shall be conducted in a manner to provide, to the maximum extent practicable, open and free competition, in accordance with federal regulations, CFR, Sec. 74.44.

D. Contractor shall have no authority to contract for, or enter into any other agreement, or on behalf of, or incur obligations on behalf of the Cal eConnect.

E. Contractor agrees to ensure that all Subcontractors are properly licensed, certified, or have valid permits for the services being provided. Copies of subcontracts, Memorandums and/or Letters of Understanding shall be on file with the Contractor and shall be made available for review at the request of Cal eConnect.

F. Contractor shall require all subcontractors to report immediately in writing to Contractor any incidents of fraud or abuse.

G. Contractor shall require language in all subcontracts to require the subcontractor to comply with all applicable state and federal laws, rules and regulations, including but not limited to the Americans with Disabilities Act (ADA) of 1990 (42 USC 12101 et. seq.) and California Government Code Sections 11135-11139.5 and all privacy, security and data protection laws, rules and regulations.

ARTICLE III. RECORDS

A. Contractor shall maintain complete records of its activities and expenditures hereunder in a form satisfactory to Cal eConnect and the State and shall make all such records available for inspection and audit by the State or federal government, and their duly authorized agents, at any time during normal business hours. These records include but are not limited to accounting records, contracts, agreements, reconciliation of the "Final Accounting Reconciliation" to the audited financial statements, letters of agreement, insurance documentation, statistical records, supporting documents, and other financial and programmatic records required to be maintained by the terms of this Agreement, or other requirements or which can reasonably be considered as pertinent to program regulations or this Agreement.

B. Length of retention period. Except as otherwise provided, records must be retained for three years from the starting date specified in paragraph (E) of this section and longer if necessary to meet one or more of the following conditions: (1) until an audit has occurred and an audit resolution has been issued or unless otherwise authorized in writing by Cal eConnect, or its designee; or (2) for such longer period as may be required by applicable statute or as Cal eConnect, or its designee deems necessary.

C. If any litigation, claim, negotiation, audit or other action involving the records has been started before the expiration of the 3-year period, the records must be retained until completion of the action and resolution of all issues which arise from it to the satisfaction of Cal eConnect and so stated in writing to Contractor, or until the end of the regular 3-year period, whichever is later.

D. To avoid duplicate record keeping, Cal eConnect may make special arrangements with the Contractor and its Subcontractors to retain any records which are continuously needed for joint use. Cal eConnect will request transfer of records to its custody when it determines that the records possess long-term retention value. When the records are transferred to or maintained by the Federal government, the 3-year retention requirement is not applicable to the Contractor or subcontractor.

E. Starting date of retention period. The retention period for the records of each funding period starts on the day the Contractor or subcontractor submits to Cal eConnect its single or last expenditure report for that period.

F. Real property and equipment records. The retention period for real property and equipment records starts from the date of the disposition or replacement or transfer at the direction of Cal eConnect.

G. Adequate source documentation of each transaction shall be maintained relative to the allowability of expenditures reimbursed by Cal eConnect under this Agreement. If the allowability of expenditures cannot be determined because records or documentation of the Contractor are nonexistent or inadequate according to Generally Accepted Accounting Principles and Procedures, the expenditures will be questioned in the audit and may be disallowed during the audit resolution process.

H. Substitution of microfilm. Copies made by microfilming, photocopying, or similar methods may be substituted for the original records.

1. If this Agreement is completely or partially terminated, the records relating to the work terminated shall be preserved and made available for the same periods as specified in above. Upon termination of this Agreement, Contractor shall ensure materials, equipment, supplies, resource directories, or other intellectual property produced under this Agreement are returned to Cal eConnect or transferred to another contractor or Subcontractor as directed by Cal eConnect.

I. Contractor agrees that Cal eConnector its designee will have the right to review, obtain, and copy all records pertaining to the performance of this Agreement. Contractor agrees to provide Cal eConnect or its designee with any relevant information requested and shall permit Cal eConnect or its designee access to its premises, upon reasonable notice, during normal business hours for the purpose of interviewing employees and inspecting and copying such books, records, accounts, and other material that may be relevant to a matter under investigation for the purpose of determining compliance with Government Code, Section 8546.7 et seq.

ARTICLE IV. ACCESS

A. Contractor shall provide access to Cal eConnect, CHHS, the Office of the National Coordinator, Department of Health and Human Services, the Controller General of the United States, or any of their duly authorized federal or State representatives to any books, documents, papers, and records of Contractor or its Subcontractors which are directly pertinent to this specific Agreement for the purpose of making an audit, examination, excerpts, and transcriptions. Contractor assures Cal eConnect that it will include this requirement in its subcontracts. Pursuant to federal regulations, the right of access in this section shall not be limited to the required record retention period but shall last as long as the records are retained.

B. Contractor agrees that Cal eConnect or their designated representative shall, at all times, have the right to review and to copy any records and supporting documentation pertaining to the performance of this Agreement.

ARTICLE V. INSURANCE

A. Contractors and its Subcontractors, other than units of local government which are similarly self-insured, must maintain adequate insurance coverage for general liability, workers' compensation liabilities, and if appropriate, auto liability including non-owned auto and/or professional liability, errors and omissions and further, Contractors and its Subcontractors shall hold Cal eConnect and CHHS harmless. Contractor shall maintain certificates of insurance for itself and all its subcontractors and monitor subcontactors to ensure the insurance requirements are met.

B. Contractor shall submit to Cal eConnect a copy of each appropriate Certificate of Insurance referencing this Agreement Number, or letter of self-insurance.

C. Contractor and its subcontractors shall be insured against liability for workers' compensation or undertake self-insurance in accordance with the provisions of the Labor Code, and Contractor affirms to comply with such provisions before commencing the performance of the work of this Agreement.

ARTICLE VI. INTELLECTUAL PROPERTY RIGHTS IN DATA AND OTHER MATERIALS

In addition to any requirements specified in federal or state law, and as required by CHITA, the Contractor shall comply with the following:

1. All work, work in progress, work product, data, trade secrets, inventions, discoveries or improvements of the techniques or programs or materials developed pursuant to this agreement, and any other tangible or intangible results prepared, produced, created, or conceived arising from, relating to, or developed in connection with the performance under this Agreement by Contractor or its employees or subcontractors ("Contractor Personnel"), either solely or jointly with others, or resulting from or suggested by any work that Contractor or Contractor Personnel may do for CHHS or Cal eConnect, or at their request, including all deliverables, papers, charts, reports and documentation, and all novel ideas, concepts,

strategies, know-how, analyses, research, techniques, inventions, processes, and improvements, patentable or unpatentable (collectively, "Deliverables" or "deliverables"), constitutes a work made for hire under the Copyright Act of 1976, 17 U.S.C. §1 et seq., and are the sole and exclusive property of CHHS or Cal eConnect. Contractor shall have no rights as to ownership, use or otherwise as to such Deliverables. Contractor shall not display, exhibit or otherwise show to any third party such Deliverables for any purpose whatsoever in any manner whatsoever (whether by inclusion in a portfolio, web site, marketing material or exhibition), without the prior written consent of CHHS or Cal eConnect.

2. Contractor agrees that if in the course of performing under this Agreement, Contractor incorporates into any Deliverable developed hereunder any invention, improvement, development, concept, discovery or other proprietary information owned by Contractor or a third party, (a) Contractor shall inform Cal eConnect, in writing before incorporating such invention, improvement, development, concept, discovery or other proprietary information into any Deliverable; and (b) Contractor hereby grants CHHS and Cal eConnect a nonexclusive, royalty-free, perpetual, irrevocable, worldwide license to use, reproduce, distribute, perform, display, prepare derivative works of, make, have made, sell and export such item as part of or in connection with such Deliverable. Contractor shall not incorporate any invention, improvement, development, concept, discovery or other proprietary information owned by any third party into any Deliverable without CHHS or Cal eConnect's prior written permission.

3. Contractor will, and will ensure that all Contractor Personnel will, communicate to Cal eConnect any and all Deliverables and will, at all times during Contractor's engagement by Cal eConnect and after Contractor's termination or expiration for any reason, assist Cal eConnect in every proper way (at Cal eConnect's expense), to obtain for its own benefit any intellectual property right for any Deliverables in the United States and any and all foreign countries, if available, by executing and delivering to Cal eConnect any and all applications, assignments, and other instruments, by giving evidence and testimony, and by executing and delivering to Cal eConnect all drawings, blueprints, notes, and specifications deemed necessary by Cal eConnect in order to apply for and obtain letters of patent of the United States or foreign countries for such Deliverables. Contractor hereby assigns and will convey to the Cal eConnect the entire right, title and interest of Contractor and Contractor Personnel in all Deliverables, including copyrights, patents and trade secrets. Contractor agrees to execute assignments and such other documents as may be requested by Cal eConnect, in a form satisfactory to Cal eConnect, evidencing, vesting and protecting CHHS or Cal eConnect's sole title and right of ownership in Deliverables. The covenants contained in this Section shall run not only in favor of CHHS and Cal eConnect, and their respective successors and assigns, and shall survive the expiration or earlier termination of this Agreement.

4. Contractor certifies that it has appropriate systems and controls in place to ensure that grant funds will not be used in the performance of this

Agreement for the acquisition, operation or maintenance of computer software in violation of copyright laws.

5. If any material funded by this Agreement is subject to copyright, CHHS and Cal eConnect reserves the right to copyright such material, and Contractor agrees not to copyright such material without prior written approval from CHHS and Cal eConnect.

6. If the material is copyrighted with the consent of CHHS and Cal eConnect, CHHS and Cal eConnect reserves a royalty-free, non-exclusive, and irrevocable license to reproduce, prepare derivative works, publish, distribute and use such materials, in whole or in part, and to authorize others to do so, provided written credit is given the author.

7. The Federal awarding agency also reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish or otherwise use, and to authorize others to use, for federal government purposes:

   i. The copyright in any work developed under a grant, sub-grant, or contract under a grant or sub-grant; and

   ii. Any rights of copyright to which a state (Contractor), sub-contractor or a contractor, purchases ownership with grant support.

B. Rights in Data, Publications or Other Materials

1. Contractor shall not spend or encumber funds covered by this Agreement on research or publications; or any activities, staff, products, or materials, including analysis and services, supporting research, and publications, unless expressly authorized by the terms of this Agreement. Contractor shall not publish any document or materials produced or resulting from activities supported by this Agreement unless the copy of the final draft for publication has been sent to the Cal eConnect, for approval, at least sixty (60) days before it is to be printed.

2. As used in this Agreement, the term “subject data” means writings, sound recordings, pictorial reproductions, drawings, designs or graphic representations, procedural manuals, forms, diagrams, workflow charts, equipment descriptions, data files and data processing or computer programs, and works of any similar nature (whether or not copyrighted or copyrightable) which are first produced or developed under this Agreement. The term does not include financial reports, cost analyses, and similar information incidental to administration of this Agreement.

3. The State and Cal eConnect may use, duplicate, or disclose in any manner and have or permit others to do so, subject to State and federal law, all subject data delivered under this Agreement.

4. Contractor is required to acknowledge the support of the federal Department of Health and Human Services, CHHS and Cal eConnect in

writing, whenever publicizing the work under this Agreement in any media. As appropriate to the materials being published or distributed, the following statement shall be included on the materials: “The conclusions and opinions expressed may not be those of the California Health and Human Services Agency (CHHS), Cal eConnect or the federal Department of Health and Human Services (DHHS). Cal eConnect’s products, services, documents and reports are federally funded for time-limited bases. As such they should be considered demonstration or pilot services. Products, services, reports and conclusions may not have been reviewed or approved by CHHS or DHHS, or Cal eConnect and do not represent the official position or endorsement of either CHHS or DHHS or Cal eConnect.”

D. **Supplemental Terms and Conditions (ARRA)**

Supplemental Terms and Conditions for Agreements using ARRA funds

1. ARRA FUNDED PROJECT: Funding for this contract has been provided through the American Recovery and Reinvestment Act (ARRA) of 2009, Pub. L. 111-5. All contractors, including both prime and subcontractors, are subject to audit by appropriate federal or State of California (State) entities. The State has the right to require that Cal eConnect, and Cal eConnect may independently determine that it shall cancel, terminate, or suspend this Agreement if Contractor or subcontractor fails to comply with the reporting, operational and other requirements contained herein.

2. ENFORCEABILITY: Contractor agrees that if Contractor or one of its subcontractors fails to comply with all applicable federal and State requirements governing the use of ARRA funds, Cal eConnect may withhold or suspend, in whole or in part, funds awarded under the program, or recover misspent funds following an audit. This provision is in addition to all other remedies available to the State under all applicable State and federal laws.

3. PROHIBITION ON USE OF ARRA FUNDS: Contractor agrees in accordance with ARRA, Section 1604, that none of the funds made available under this contract may be used for any casino or other gambling establishment, aquarium, zoo, golf course, or swimming pools.

4. REQUIRED USE OF AMERICAN IRON, STEEL AND OTHER MANUFACTURED GOODS: Contractor agrees that in accordance with ARRA, Section 1605, neither Contractor nor its subcontractors will use ARRA funds for a project for the construction, alteration, maintenance, or repair of a public building or public work unless all of the iron, steel and manufactured goods used in the project are produced in the United States or in a manner consistent with United States obligations under international agreements, as further defined in Code of Federal Regulations (CFR) Title II, Part 176. The Contractor understands that this requirement may only be waived by the applicable federal agency in limited situations as set out in ARRA, Section 1605 and applicable federal regulations.

5. WAGE RATE REQUIREMENTS: In accordance with ARRA, Section 1606, the Contractor assures that it and its sub-recipients shall fully comply with said Section and notwithstanding any other provision of law and in a manner consistent with other provisions of ARRA, all laborers and mechanics employed by contractors and subcontractors on projects funded directly by or assisted in whole or in part by and through the federal government pursuant to ARRA shall be paid wages at rates not less than those prevailing on projects of a character similar in the locality as determined by the United States Secretary of Labor in accordance with Subchapter IV of Chapter 31 of Title 40, United States Code (Davis-Bacon Act). It is understood that the Secretary of Labor has the authority and functions set forth in Reorganization Plan Numbered 14 or 1950 (64 Stat. 1267; 5 U.S.C. App.) and Section 3145 of Title 40, United States Code.

6. INSPECTION OF RECORDS: In accordance with ARRA Sections 902, 1514 and 1515, Contractor agrees that it shall permit the State of California, the United States Comptroller General or his representative or the appropriate Inspector General appointed under Section 3 or 8G of the United States Inspector General Act of 1978 or his representative to: (1) examine any records that directly pertain to, and involve transactions relating to, this contract; and (2) interview any officer or employee of Contractor or any of its subcontractors regarding the activities funded with funds appropriated or otherwise made available by the ARRA. Contractor shall include this provision in all of the contractor's agreements with its subcontractors from whom the contractor acquires goods or services in its execution of the ARRA funded work.

7. WHISTLEBLOWER PROTECTION: Contractor agrees that both it and its subcontractors shall comply with Section 1553 of the ARRA, which prohibits all non-federal employers, including the State, and all contractors of the State, from discharging, demoting or otherwise discriminating against an employee for disclosures by the employee that the employee reasonably believes are evidence of: (1) gross mismanagement of a contract relating to ARRA funds; (2) a gross waste of ARRA funds; (3) a substantial and specific danger to public health or safety related to the implementation or use of ARRA funds; (4) an abuse of authority related to implementation or use of ARRA funds; or (5) a violation of law, rule, or regulation related to an agency contract (including the competition for or negotiation of a contract) awarded or issued relating to ARRA funds. Contractor agrees that it and its subcontractors shall post notice of the rights and remedies available to employees under Section 1553 of Title XV of Division A of the ARRA.

8. FALSE CLAIMS ACT: Contractor agrees that it shall promptly notify the State and shall refer to an appropriate federal inspector general any credible evidence that a principal, employee, agent, subcontractor or other person has committed a false claim under the False Claims Act or has committed a criminal or civil violation of laws pertaining to fraud, conflict of interest, bribery, gratuity, or similar misconduct involving ARRA funds.

9. REPORTING REQUIREMENTS: Pursuant to Section 1512 of the ARRA, in order for state agencies receiving ARRA funds to prepare the required reports, Contractor agrees to provide Cal eConnect with the following information on a quarterly basis or upon request:

   a. The total amount of ARRA funds received by Contractor during the Reporting Period;

   b. The amount of ARRA funds that were expended or obligated during the Reporting Period;

   c. A detailed list of all projects or activities for which ARRA funds were expending or obligated, including:

      i. The name of the project or activity;

      ii. A description of the project or activity;

      iii. An evaluation of the completion status of the project or activity; and

      iv. An estimate of the number of jobs created and /or retained by the project or activity;

   d. For any contracts equal to or greater than $25,000:

      i. The name of the entity receiving the contract;

      ii. The amount of the contract;

      iii. The transaction type;

      iv. The North American Industry Classification System (NAICS) code or Catalog of Federal Domestic Assistance (CFDA) number;

      v. The Program source;

      vi. An award title descriptive of the purpose of each funding action;

      vii. The location of the entity receiving the contract;

      viii. The primary location of the contract, including the city, state, congressional district and country;

      ix. The DUNS number, or name and zip code for the entity headquarters;

x. A unique identifier of the entity receiving the contract and the parent entity of Contractor, should the entity be owned by another; and

xi. The names and total compensation of the five most highly compensated officers of the company if it received: 1) 80% or more of its annual gross revenues in Federal awards; 2) $25M or more in annual gross revenue from Federal awards and; 3) if the public does not have access to information about the compensation of senior executives through periodic reports filed under section 13(a) or 15(d) of the Securities Exchange Act of 1934 or section 6104 of Internal Revenue Code of 1986.;

e. For any contracts of less than $25,000 or to individuals, the information required above may be reported in the aggregate and requires the certification of an authorized officer of Contractor that the information contained in the report is accurate.

f. Any other information reasonably requested by the State of California or required by state or federal law or regulation.

g. Standard data elements and federal instructions for use in complying with reporting requirements under Section 1512 of the ARRA, are to be provided online at www.FederalReporting.gov. Any additional or amended reporting requirements are hereby added to this Agreement by this reference.

E. **Financial Matters**

1. Payment: Payment shall not be due until the later of: (i) the date of Acceptance of Deliverables or Services; or (ii) receipt of an accurate invoice.

Payment to Contractor is contingent upon Cal eConnect receiving funding from the State of California and the Supplemental Terms and Conditions described in Section D. Cal eConnect shall bear no liability or responsibility for payment to Contractor, even for services provided and delivered, in the event payment to Cal eConnect from the Federal, State or local government is delayed, suspended, or terminated.

Payment to the Contractor will be contingent upon final approval of each deliverable. The Contractor may invoice Cal eConnect only after the successful completion and acceptance of the deliverable. The Contractor may not invoice Cal eConnect for any costs exceeding the maximum amount identified to complete a deliverable.

2. Invoices: Upon Acceptance of a Deliverable, invoices shall be submitted the month following the month in which the Deliverable was accepted. Contractor shall not submit invoices more frequently than monthly.

In no event shall Contractor submit invoices later than one year following the date charges were incurred. Cal eConnect will not pay any invoice submitted more than one year after the date charges were incurred.

Contractor must submit an original invoice which shall specify the amount due and in which Contractor has certified that Services required under this Contract conform to the requirement set forth in this Contract. In addition, Contractor shall provide an electronic copy (in a commercially standard format) of each invoice submitted. Invoices payable by Cal eConnect shall be submitted to:

Cal eConnect
Attn: Accounting Office
1900 Powell Street, Suite 1000
Emeryville, CA 94608

a. Cal eConnect Approval: All invoices submitted must meet with the approval of Cal eConnect prior to payment.

b. Inclusion of Contract Number: All invoices, bills of lading, shipping memos, packages and any other form of correspondence shall refer to this Contract by number plus any unique identifier generated by Cal eConnect on a Work Authorization.

c. Information Required: Invoices shall account for each billable item, description and cost. Additional invoice descriptions may be mutually agreed upon by Cal eConnect and Contractor.

d. Incorrect Invoices: Contractor shall make every effort to reconcile incorrect invoices in a timely manner, not to exceed 30 days from Notice by Cal eConnect of a discrepancy. Cal eConnect shall withhold payments for disputed amounts from invoices until the discrepancies have been resolved.

e. Work Authorizations: Work Authorizations shall be billed monthly in arrears, using the rates provided in Attachment 2, Cost Sheet**.** No invoice for Work Authorizations will be due and payable by Cal eConnect until Acceptance of the Services provided.

f. Invoicing of Post Implementation Services: Each calendar month of the Post Implementation Phase, following Cal eConnect Acceptance of System, Contractor may submit an invoice for payment of the Services provided that month. Monthly billings to Cal eConnect shall be based on the Service costs in Attachment 2, Cost Sheet.

3. No Increases: Contractor shall not increase the amounts due from Cal eConnect under this Contract for all Services and Deliverables as described in Attachment 2, Cost Sheet, except those increases that may result from Work Authorizations agreed to by Cal eConnect and

Contractor in accordance with Section H.3 Unanticipated Tasks of the Contract.

4. Transportation Costs and Other Fees or Expenses: No charge for delivery, drayage, express, parcel post, packing, cartage, insurance, license fees, permits, cost of bonds, or for any other purpose will be paid by Cal eConnect unless expressly included and itemized in the Contract.

5. Taxes: The prices listed in [Attachment 2, Cost Sheet] include all applicable Federal, State, and local taxes and duties in existence as of the date this Contract is executed.

6. Contractor Expenses: The consideration to be paid Contractor, as provided herein, shall be in compensation for all of Contractor's and its Subcontractors' expenses incurred in the performance hereof, including without limitation travel and per diem, unless otherwise expressly agreed to in writing by Cal eConnect prior to the expenditure of such funds.

7. Most Favored Customer: Should Contractor, following the Execution Date, agree to provide similar Services to any other customer for a fee or price (hereinafter "prices") more favorable than the prices specified in this Contract, then Cal eConnect shall be permitted the benefit of such more favorable prices as of the date such prices became available in such other agreement.

8. Overpayments to Contractor: Contractor shall promptly refund to Cal eConnect the full amount of any erroneous payments, incorrect payments or overpayments upon determination by Contractor or upon receipt of Notice from Cal eConnect.

9. Credits and Right to Set Off: Any credits due Cal eConnect under this Contract may be applied against Contractor's invoices with appropriate information attached, upon giving of prior Notice required herein, if any, by Cal eConnect to Contractor. Cal eConnect shall have the right to set off any amounts owed to Contractor against any damages or charges assessed by Cal eConnect against Contractor.

10. Advance Payments Prohibited: No payments in advance of or in anticipation of Services or Equipment to be supplied under this Contract shall be provided by Cal eConnect.

11. Payments to Subcontractors: Money paid to Contractor by Cal eConnect shall be dispersed to its subcontractors after receipt of the money in accordance with the terms of the applicable subcontract. Upon final payment to Contractor, full payment to the Subcontractors shall be made, provided that there are no bona fide disputes over the Subcontractor's performance under such subcontract.

12. Reduction in Price: If there is a reduction in the work or Services provided to Cal eConnect by Contractor there shall be a corresponding reduction in the price Cal eConnect pays to Contractor for such work or Services.

13. In the event of a conflict between the terms of this Section E Financial Matters and those of the Section G.5 Acceptance of Software, the latter will govern.

F. **Deliverables**

1. The Contractor shall develop and deliver all Deliverables listed in Attachment 1, Statement of Work, and all Deliverables listed in the Project Management Plan pursuant to the Statement of Work.

2. Deliverable Acceptance Criteria: All concluded work must be submitted to Cal eConnect's PMO for review and approval or rejection. It will be Cal eConnect's sole determination as to whether a deliverable has been successfully completed and is acceptable.

   Throughout the Contract, Cal eConnect will review and validate deliverables prior to final acceptance. In addition, Cal eConnect's PMO will verify and approve the Contractor's deliverable invoices. Signed acceptance is required from the Cal eConnect PMO to approve an invoice for payment.

   Deliverable acceptance criteria consist of the following:

   i. Deliverable-specific work was completed as specified and the final deliverable product/service was rendered.

   ii. Plans, schedules, designs, documentation, and reports (deliverables) were completed as specified and approved.

   iii. All deliverable documentation and artifact gathering have been completed.

   iv. All deliverables are in a format useful to Cal eConnect.

   v. If a deliverable is not accepted, Cal eConnect will provide the reason, in writing, within ten business days of receipt of the deliverable.

G. **Software Special Provisions**

1. License Grant

   a. Contractor hereby grants to Cal eConnect and the State, and Cal eConnect accepts from Contractor, subject to the terms and conditions of this Contract, a worldwide, perpetual non-exclusive, non-transferable license to use the Software Products listed in Statement of Work of this Contract, and their respective documentation, manuals and updates, upgrades, and enhancements (hereinafter referred to as "Software Products").

b. Cal eConnect may use the Software Products in the conduct of its own business, that of the State, and any division thereof.

c. The license granted above authorizes Cal eConnect and the State to use the Software Products in machine-readable form on the Computer System being used, by the Contractor, to host the Provider Directory Services with eHIE Capabilities System. Said Computer System and its associated units (collectively referred to as CPU) are hosted and maintained by Contractor, as designated in the Statement of Work.

d. By prior written notice, Cal eConnect may redesignate the CPU in which the Software Products are to be used. The redesignation will be effective upon the date specified in the notice of redesignation.

2. Encryption/CPU ID Authorization Codes

a. When Encryption/CPU Identification (ID) authorization codes are required to operate the Software Products, the Contractor will provide all codes to Cal eConnect with delivery of the Software Products.

b. When changes in designated CPUs occur, Cal eConnect will notify the Contractor via telephone and/or facsimile/e-mail of such change. Upon receipt of such notice, Contractor will issue via telephone and/or facsimile/e-mail to Cal eConnect within 24 hours, and at no additional charge, a temporary encryption ID authorization code for use on the newly designated CPU until such time as a permanent code is assigned.

3. Fees and Charges: Upon acceptance of Software Products by Cal eConnect, in accordance with Paragraphs 5 herein and the Statement of Work, Cal eConnect will pay the license fee or recurring charge for the Software Products as set forth in Statement of Work. Charges will commence on the Acceptance Date as established in the Statement of Work. The Contractor shall render invoices for recurring charges or single charges in the month following the month in which the charges accrue.

4. Maintenance: The following terms and conditions are superseded and replaced by any alternate or inconsistent terms and conditions in the Statement of Work.

a. The correction of any residual errors in any Software Product that may be discovered by Contractor or by Cal eConnect will be considered maintenance. Such maintenance will be performed by Contractor without additional charge for the duration of this contract. Suspected errors discovered by Cal eConnect in the Software Products will be handled by the following procedures:

i. A listing of the output and a copy of the identical input data in machine-readable form will be submitted to Contractor along with a completed copy of the appropriate Contractor information form and, if appropriate, a listing of the contents of the memory of the CPU at the time the error condition was noted.

ii. Errors in the Software Product as verified by Contractor will be corrected by providing a new copy of said Software Product (or of the affected portions) in machine-readable form.

iii. The Contractor shall correct Software Product errors, at no additional charge, within a reasonable time as mutually agreed by the parties.

5. Acceptance of Software

a. Commercial Software: Acceptance of Commercial Software will be governed by the terms and conditions of the license agreement governing such Software as mutually agreed by the parties. Cal eConnect needs to pre-approve the list of Commercial Software and open source software used in the performance of the Contract.

b. Custom Software: Unless otherwise provided in the Statement of Work, acceptance procedures for Custom Software will be as set forth in this subsection (b). Cal eConnect shall be deemed to have accepted each Custom Software Product upon its issuance of written notice of such acceptance (collectively, “Acceptance”). No payment for Custom Software will be due before Acceptance thereof, except to the extent required by progress payment terms in the Statement of Work. Any notice of rejection will explain how the Custom Software Product fails to conform to the functional and performance specifications of this Contract. Contractor will, upon receipt of such notice, investigate the reported deficiency and remedy it promptly. Cal eConnect, in its sole discretion, will have the option to re-perform the acceptance test. If the Contractor is unable to remedy the deficiency within (60) days of notice of rejection, Cal eConnect shall have the option of accepting substitute Software, terminating for default the portion of the Contract that relates to such Custom Software, or terminating this Contract in its entirety for default.

6. Right To Copy or Modify

a. Any Software Product provided by Contractor in machine-readable form may be copied, in whole or in part, in printed or machine-readable form for use by Cal eConnect with the designated CPU, to perform one-time benchmark tests, for archival or emergency restart purposes, to replace a worn copy, to understand the contents of such machine-readable material, or to modify the Software Product as provided below; provided, however, that no more than the number of printed copies and machine-readable copies as specified in the Statement of Work will be in existence under this Contract at any one time without prior written consent from Contractor. Such consent shall not be unreasonably withheld by the Contractor. The original of Custom Software, and any copies of such software, in whole or in part, which are made hereunder shall be the property of Cal eConnect as work made for hire.

b. Cal eConnect agrees to keep any such copies and the original at a mutually designated Cal eConnect location, except that Cal eConnect may transport or transmit a copy of the original of any Software Product to another location for backup use.

c. Cal eConnect may modify any non-personal computer Software Product, in machine-readable form, for its own use and merge it into other program material; provided that nothing in this sub-section c) will be construed to contradict the terms of any separate applicable third party license agreement. Any portion of the Software Product included in any merged program material shall be used only on the designated CPUs and shall be subject to the terms and conditions of this Contract.

7. Future Releases: Unless otherwise specifically provided in this Contract, or the Statement of Work, if improved versions of any Software Product are developed by Contractor, and are made available to other licensees, they will be made available to Cal eConnect at Cal eConnect's option at a price no greater than the Contract price plus a price increase proportionate to the increase from the list price of the original version to that of the new version, if any. If the Software Product has no list price, such price increase will be proportionate to the increase in average price from the original to the new version, if any, as estimated by the Contractor in good faith. In no event shall Cal eConnect pay more for such future releases or improved versions than any other licensee.

8. Technology Escrow. Contractor agrees to place a copy of the source code, computed objects, design specifications and documentation, and technical documents for each Software Product in escrow with an independent third party escrow agent, to enter into a three-party escrow agreement in a form which will be mutually agreed to by the parties (the "Escrow Agreement") with Cal eConnect and the escrow agent, and to promptly update the escrowed materials so that the escrowed materials correspond with the current release of the Software Products then used by Cal eConnect. Cal eConnect shall have the right to obtain such escrowed materials in accordance with the terms of the Escrow Agreement.

9. Service Level Warranties: Contractor represents and warrants that each product and service provided hereunder will function and perform in

accordance with the service levels which will be mutually agreed to by the parties (the “Service Levels”). The Service Levels shall be monitored, tracked, measured and reported on a monthly basis. If the Service Levels are not met, Contractor shall engage with Cal eConnect in corrective actions and determination of root cause. Any variation from the Service Level may produce a service credit that will be calculated based on the failure to achieve the metric over time. Penalties or credits will be assessed for failure to meet the Service Levels.

10. Training Warranties: The Agreement shall provide for all training of Cal eConnect, CHHS and their respective employees and agents, to allow such individuals to make full use of the products and services provided under the Agreement, including any retraining or training for any updates or upgrades to Software Products. All training provided to such persons shall be performed in a timely, professional and workmanlike manner by Contractor’s trainers with appropriate education and experience qualifications. Training will be conducted at facilities of Cal eConnect, or such other location as may be designated by Cal eConnect, during regular business hours of Cal eConnect.

H. Personal Services Special Provisions

1. Personnel

a. Contractor personnel shall perform their duties during regular work days and normal work hours of Cal eConnect, except as may be specifically agreed to otherwise by Cal eConnect.

b. Cal eConnect reserves the right to disapprove the continuing assignment of Contractor personnel provided to Cal eConnect under this Contract. If Cal eConnect exercises this right, and the Contractor cannot immediately replace the disapproved personnel, the parties agree to proceed with any equitable adjustment in schedule or other terms that may be affected thereby.

c. The Contractor will make every effort consistent with sound business practices to honor the specific requests of Cal eConnect with regard to assignment of its employees; however the Contractor reserves the sole right to determine the assignment of its employees. If a Contractor employee is unable to perform due to illness, resignation, or other factors beyond the Contractor’s control, the Contractor will use best efforts to provide suitable substitute personnel within ten (10) business days.

d. In recognition of the fact that Contractor personnel providing services under this Contract may perform similar services from time to time for others, this Contract shall not prevent Contractor from performing such similar services or restrict Contractor from using the personnel provided to Cal eConnect under this Contract, providing that such use does not conflict with the performance of services under this Contract or breach Contractor's obligations hereunder with respect to confidentiality and security of data.

e. Contractor shall provide a project manager who will be assigned for the duration of the project.

2. Responsibilities of Cal eConnect

a. Cal eConnect is responsible for providing reasonably required information, data, documentation, and test data to facilitate the Contractor's performance of the work, and will provide such additional assistance and services as is specifically set forth in the Statement of Work.

b. The Contractor will not be responsible for any delay or cost increase, to the extent that it is demonstrated to be directly caused by Cal eConnect's failure to fulfill responsibilities set forth herein. In the event of any claim for equitable adjustment to price, schedule, or both, the parties will negotiate in good faith regarding execution of a Contract amendment. Should the Contractor determine that a delay exists due to a failure of Cal eConnect, the Contractor will promptly notify Cal eConnect in writing.

3. Unanticipated Tasks

a. In the event that additional work must be performed which was wholly unanticipated and is not specified in the Statement of Work, but which in the opinion of both parties is necessary to the successful accomplishment of the general scope of work outlined, the procedures outlined in this Section will be employed.

b. For each item of unanticipated work not specified in the Statement of Work, a Work Authorization will be prepared in accordance with the sample attached as Exhibit A.

c. It is understood and agreed by both parties to this Contract that all of the terms and conditions of this Contract shall remain in force with the inclusion of any such Work Authorization. Such Work Authorization shall in no way constitute a Contract other than as provided pursuant to this Contract nor in any way amend or supersede any of the other provisions of this Contract unless expressly stated by Cal eConnect.

d. Each Work Authorization shall consist of a detailed statement of the purpose, objective, or goals to be undertaken by the Contractor, the job classification or approximate skill level of the personnel to be made available by the Contractor, an identification of all significant material to be developed by the Contractor and delivered to Cal eConnect, an identification of all significant materials to be delivered by Cal eConnect to the Contractor, an estimated time schedule for the provisions of these services by the Contractor, completion criteria for the work to be performed, the name or identification of the Contractor personnel to be assigned, the Contractor's estimated work hours required to accomplish the purpose, objective or goals, the Contractor's billing rates per work hour, and the Contractor's estimated total cost of the Work Authorization. Contractor shall base prices for Work Authorizations on the reasonable number of Staff hours required multiplied by the Change Order Rates listed in Attachment 2, Cost Sheet, plus any other reasonable costs to be incurred to effect the change at a fair and reasonable price.

e. All Work Authorizations must be in writing prior to beginning work and signed by the Contractor and Cal eConnect.

f. Cal eConnect has the right to require the Contractor to stop or suspend work on any Work Authorization pursuant to Section A.44 Stop Work.

g. Personnel resources will not be expended (at a cost to Cal eConnect) on task accomplishment in excess of estimated work hours required unless the procedure below is followed:

i. If, in the performance of the work, the Contractor determines that a Work Authorization to be performed under this Contract cannot be accomplished within the estimated work hours, the Contractor will immediately notify Cal eConnect in writing of the Contractor's estimate of the work hours which will be required to complete the Work Authorization in full. Upon receipt of such notification, Cal eConnect may:

(a) Authorize the Contractor to expend the estimated additional work hours or service in excess of the original estimate necessary to accomplish the Work Authorization (such an authorization not unreasonably to be withheld), or

(b) Terminate the Work Authorization, or

(c) Alter the scope of the Work Authorization in order to define tasks that can be accomplished within the remaining estimated work hours.

ii. Cal eConnect will notify the Contractor in writing of its election within seven (7) calendar days after receipt of the Contractor's notification. If notice of the election is given to proceed, the Contractor may expend the estimated additional work hours or services. Cal eConnect agrees to reimburse the Contractor for such additional work hours.

4. Service Warranties.

a. Contractor represents and warrants that the services provided hereunder will be performed in a timely, skillful, professional, diligent and workmanlike manner by competent personnel, including training personnel, familiar with the subject matter to which such person is assigned. In addition, the services shall conform to or exceed the standard generally observed in the industry for similar services and will be performed in a manner that will cause minimal interference with Cal eConnect ongoing business operations.

b. Contractor shall, without charge, reperform the services, replace any material and correct any quality of work found by Cal eConnect not to conform to the requirements set forth in the Agreement.

EXHIBIT A – WORK AUTHORIZATION SAMPLE

WORK AUTHORIZATION

TITLE: Financial Report Development

Task Summary:
Develop program to format and print simulated 70/752 displays using a sequential data set as input.

Schedule Dates:
Start Date: April 2, 2007
Completion Date: April 30, 2007

Estimated Labor-Hours Labor-Hour Rate Estimated Total Cost

#	Contractor Personnel to Be Assigned	Job Classification/ Skill Level	Estimated Labor-Hours	Labor-Hour Rate	Estimated Total Cost
1.	Jane Doe	Programmer Analyst	100	$90.00	$9,000.00
2.					
	Totals		**100**	**$90.00**	**$9,000.00**

Completion Criteria:
Acceptance of work by Cal eConnect.

This task will be performed in accordance with this Work Authorization and the provisions of Contract Number “TBD”.

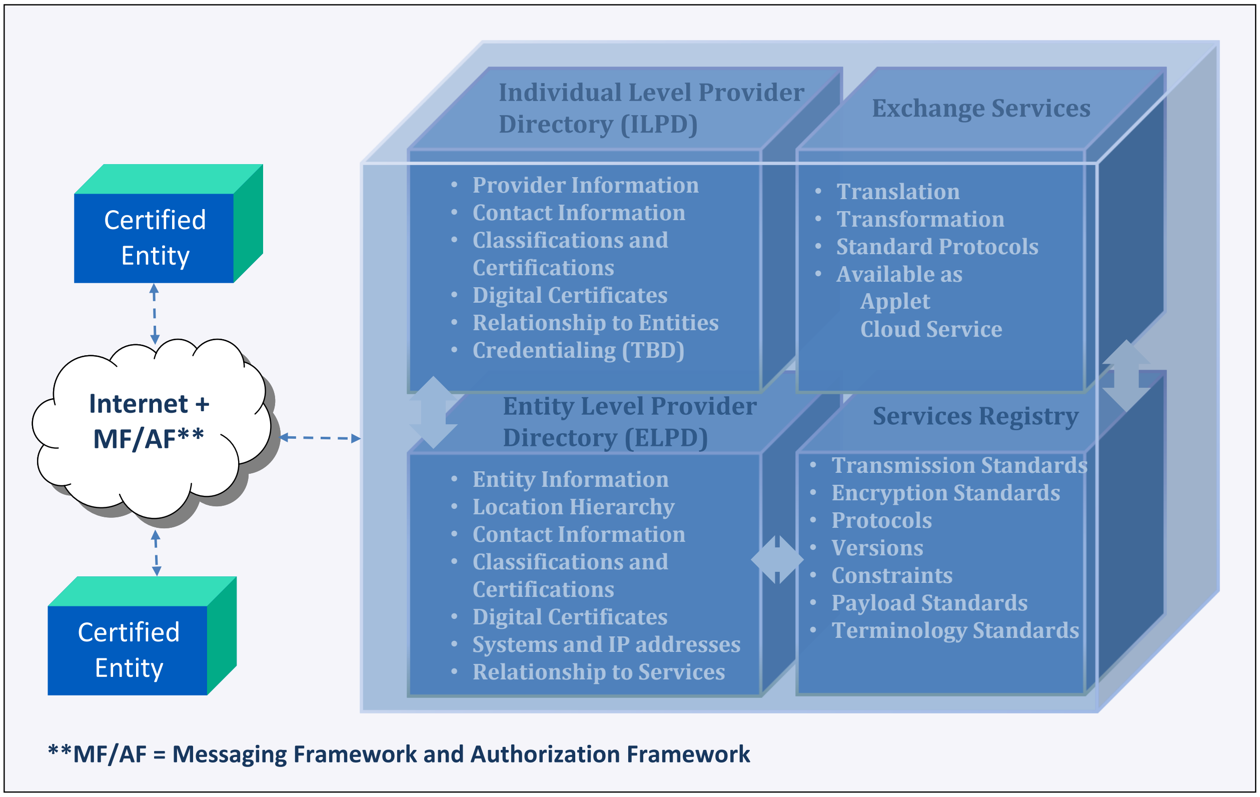
Approval

______________________________ _______________________________
Contract Project Manager Cal eConnect Project Manager

EXHIBIT B – FUNCTIONAL AND TECHNICAL CRITERIA

This Exhibit B is a guideline for understanding, at a more detailed level where required, the functional requirements described in Section III.B of the Scope of Work. Bidders do not need to propose the same architecture or necessarily respond to the detailed functions described in this Exhibit B unless it is necessary to be compliant with the description of the Critical Functions in the Scope of Work.

Figure 1 High-level overview of the Cal eConnect Infrastructure



1. *Messaging Framework*

The Messaging Framework is a set of specifications that define the default format and contents for information exchange within the Cal eConnect infrastructure. Senders and receivers of HIE transactions may use the Messaging Framework when transmitting health information or making requests for health information (although they may also use other messaging models, such as NwHIN Direct or NwHIN Exchange). Client applications that access the Entity Level Provider Directory or the Individual Level Provider Directory via their web-services APIs *must* use the Messaging Framework.

Note: The vendor who develops the core services of the Cal eConnect Infrastructure will be expected to implement the messaging framework for two purposes:

1. To enable client applications to interact with the ILPD and ELPD via a programmatic (web services) API, as described in Section 3 and Section 6. For example, an EHR may access the ILPD to enable its users to discover Providers listed therein when initiating a

health information exchange and access the ELPD to correctly address and format the messages sent to those Providers.

2. To develop a client application that can serve both as a test harness for interacting with the ILPD and ELPD and as a basic tool for securely sending and receiving health information when Providers lack other means to do so.

1.1. Functional Requirements

The messaging framework defines an asynchronous messaging protocol that meets four requirements:

1. It is based on non-proprietary industry standards
2. It can operationalize the security and trust models defined for secure exchange of health information in California
3. It can provide secure transport of health information over the public internet
4. It supports the types of transaction required to achieve meaningful use

1.1.1. "Push" Message Pattern

Based on the Stage-1 meaningful use requirements, the first priority of the messaging framework will be to support a "push" message pattern. In this pattern, unsolicited transmissions of patient-specific health information are pushed from one provider to another, and appropriate acknowledgements are returned to indicate the action taken upon receipt of the message. The push message pattern shall also be used by providers and entities to write information to the ILPD and ELPD via web-services interfaces.

Transaction Types: The minimum set of transaction types that must be supported by the "push" message pattern includes

- Deliver Laboratory Test Result to Ordering Provider and Copied Provider(s)
- Deliver Laboratory Test Result to Public Health Agency
- Send Hospital Discharge Summary
- Send Ambulatory Patient Summary from One Provider to Another
- Send Immunization Event to an Immunization Registry
- Send Patient Data to a PHR
- Send Insurance Claim to a Payer
- Send Secure Message to a Provider
- Write Record(s) to Entity Level Provider Directory
- Write Record(s) to Individual Level Provider Directory

Push-Pattern Messaging Handshake: The basic handshake for transmitting an unsolicited message from Provider-1 using Node-1 to Provider-2 using Node-2 is:

1. Provider-1 initiates transmission of a message from his messaging gateway (Node-1) to the messaging gateway designated for Provider-2 (Node-2)
2. Node-1 establishes a network connection to Node-2 over the public internet. This connection is secured via TLS (including mutual authentication and exchange of encryption key(s))
3. Node-1 transmits the message to Node-2 over this secure channel
4. Node-2 acknowledges receipt of the message over this secure channel (acknowledgement signifies that the message was conformant to the specifications of the messaging framework; it does not signify that the transmitted health information was received by Provider-2 or was accepted)
5. The secure channel is closed
6. Node-2 delivers the message to Provider-2 such that Provider-2 can review it and take appropriate action. If Node-2 is Provider-2's own information system, this processing may entail simply queuing the message in Provider-2's "in-box." If Node-2 is a messaging intermediary that is also part of the Cal eConnect Infrastructure, this processing may entail forwarding the message to the recipient's node using the same messaging framework and push-pattern handshake. If Node-2 is a messaging intermediary that routes messages only within Provider-2's institution, this processing may entail forwarding the message to Provider-2's information system using any secure and reliable network.
7. Provider-2 reviews and acts upon the message. Based on the action taken, Provider-2 formulates an acknowledgement message for the sending provider. The message will be sent from Provider-2's messaging gateway (Node-2) to the return address indicated for Provider-1 (Node-1). The acknowledgement message will contain one of several acknowledgements specific to the type of information originally sent and the disposition of that information, such as:
    - Data Received and Accepted
    - Data Received and Not Accepted – Authorization Failure
    - Data Received and Not Accepted – Patient-Matching Failure
    - Data Received and Not Processed – Timeout (data was received but not acted upon within a specified time period)
    - …etc.
8. Node-2 establishes a secure network connection to Node-1 and transmits the acknowledgement message per steps 2 through 5 above.

1.1.2. "Pull" Message Pattern

A query/response ("pull") message pattern will be required to retrieve information from the Entity Level Provider Directory and Individual Level Provider Directory via web-services interfaces. In addition, a query/response pattern for exchanging PHI may be required to enable providers to fulfill the stage-2 and stage-3 meaningful-use criteria. In this pattern, a request for patient-specific health information is transmitted from one provider to another, and the requested information and/or an appropriate acknowledgement is returned to the initiating provider.

Transaction Types: The minimum set of transaction types that must be supported by the "pull" message pattern includes:

- Request Hospital Discharge Summary
- Request Ambulatory Patient Summary
- Request Immunization History
- Request Eligibility Information from a Payer
- Request Patient Information from a PHR
- Request Record(s) from Entity Level Provider Directory
- Request Record(s) from Individual Level Provider Directory

Pull-Pattern Messaging Handshake: The basic handshake for executing a query/response transaction initiated by Provider-1 using Node-1 and fulfilled by Provider-2 using Node-2 is:

1. Provider-1 initiates transmission of a request message from his messaging gateway (Node-1) to the messaging gateway designated for Provider-2 (Node-2)
2. <Steps 2 – 6 are identical to steps 2-6 for the "push" message pattern.>
7. Provider-2 reviews and acts upon the request. Based on the action taken, Provider-2 formulates an acknowledgement message for the sending provider. The message will be sent from Provider-2's messaging gateway (Node-2) to the return address indicated for Provider-1 (Node-1). The response will contain one of several acknowledgements specific to the type of information originally requested and the disposition of the request, such as:
    - Request Received and Accepted – Information Attached
    - Request Received and Accepted – Information Pending (will be sent in a forthcoming message)
    - Request Received and Not Accepted – Authorization Failure
    - Request Received and Not Accepted – Patient-Consent Failure
    - Request Received and Not Accepted – Patient-Matching Failure
    - Request Received and Not Processed – Timeout (request was received but not acted upon within a specified time period)
8. Node-2 establishes a secure network connection to Node-1 and transmits the message per steps 2 through 8 of the "push" pattern above (including an acknowledgement from the original requestor that the information was received and accepted).

1.1.3. "Publish/Subscribe" Message Pattern

The publish/subscribe message pattern is intended to support a future messaging model in which Providers will subscribe to information feeds from other Providers. For example, this model will enable a primary care physician to receive visit summaries from a specialist to whom she has referred a patient for multiple visits without requiring the primary care physician to request such summaries each time the patient is seen.

This message pattern is a variation of the "pull" message pattern in which Provider-1 issues to Provider-2 a standing request ("subscription") for information of a specific type regarding a specific patient. It is the responsibility of Provider-2's information system to maintain a record of the request and to "push" the requested information (without prompting) whenever it becomes available. Depending on the implementation of this message pattern, Provider-2 may push the information directly to Provider-1, or Provider-2 may push the information to an intermediary message-routing service that maintains a record of all the providers who have subscribed to the specific information (to be determined). In either case, the technical specifications of the Messaging Framework and Authorization Framework should support this message pattern.

1.1.4. Unique Identifiers for Transmitted Messages

The Messaging Framework shall require that each transmitted message include a globally unique "message ID" that should be referenced in subsequent responses to the message, recorded in audit logs, etc. The generation, format, and placement of this ID within messages are technical details that shall be specified by the responding vendor. For example, the ID could be a GUID generated by the sending system and transmitted within the SOAP header of each message.

1.2. Technical Specifications

The messaging framework will use SOAP messages transmitted over HTTP with Transport Layer Security (TLS). More specifically, the framework will conform to the WS-I Basic Profile 2.0[i] and the WS-I Security Profile 1.1[ii]. These profiles use the web-services standards specified in Table 1.1, but prescribe further constraints to improve interoperability among conforming systems.

Table 1.1. Standards specified by WS-I Basic Profile 2.0 and WS-I Security Profile 1.1

Specification	Version	Comments
SOAP	1.2	
SOAP Message Encoding Style = Document Literal		
XML Schema	1.0	
WSDL	1.1	
HTTP	1.1	
Transport Layer Security (TLS)	1.0	
Advanced Encryption Standard (AES) with 128-bit key length		Symmetric encryption algorithm
Secure Hash Algorithm 1 (SHA-1)		Verification of message integrity in TLS

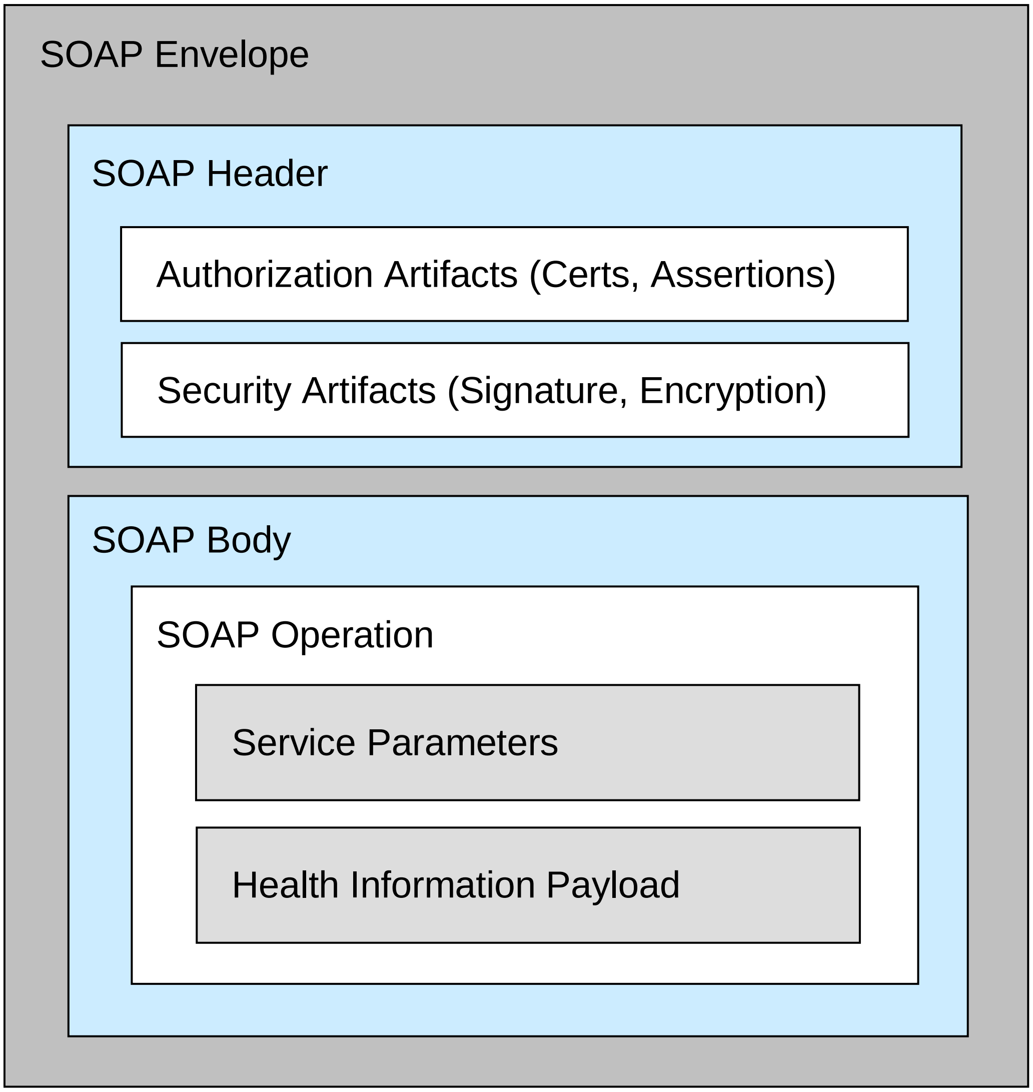
X.509 Token Profile	1.0	Digital certificates for nodes communicating via TLS

Note that these specifications are consistent with the messaging platform specifications for NwHIN-Exchange[iii] as well as the transport and security requirements for EHR certification per the ONC Final Rule for EHR certification[iv].

1.2.1. General Message Structure

Figure 3.1 summarizes the general structure of SOAP messages specified by the messaging framework. The details of this structure will be prescribed by the WS-I Basic Profile 2.0 and the WS-I Security Profile 1.1, as well as additional constraints specified by the vendor providing the infrastructure.

Figure 1.1 Schematic of message structure for Messaging Framework


SOAP Envelope
SOAP Header
Authorization Artifacts (Certs, Assertions)
Security Artifacts (Signature, Encryption)
SOAP Body
SOAP Operation
Service Parameters
Health Information Payload

1.2.1.1. Authorization Artifacts

This section contains the digital certificate of the sending entity, the digital certificate of the sending Provider, and the authentication and authorization assertions for the sending Provider. These artifacts are further described in Section 2.

1.2.1.2. Content-Security Artifacts

This section contains the digital signature for the SOAP body, to verify that the service parameters and health information payload were not altered during the message's transit (required). The signature method is specified in Section 1.2.2. The section may also contain WS-Security headers required for the encryption of the health information payload (optional). The encryption method, if one is used, is specified in Section 1.2.2.

1.2.1.3. SOAP Operation

This section contains the name of the operation that the message is intended to perform and the parameters and health information contents related to that operation. For example, SOAP Operations for the "push" message pattern may be entitled "SendPushPatternMessage" and "AcknowledgePushPatternMessage".

1.2.1.4. Service Parameters

These data elements provide meta-information about the intended operation, including:

1. The identifier of the intended recipient ("TO" address).
2. The identifier of the sender of the message ("FROM" address)
3. The identifier of the transaction type being requested (e.g., "SendDischargeSummary", "RequestImmunizationHistory")
4. The unique identifier of the protocol being used to conduct the transaction, as specified in the Services Registry
5. The return address for responses to the transmitted messages, whether acknowledgement messages or the requested patient information

The contents of this section are never encrypted, because they may be required by messaging intermediaries and message-processing systems to correctly route and process incoming HIE messages. These contents may not, therefore, contain any protected health information.

1.2.1.5. Health Information Payload

This section contains all of the protected health information communicated in the message. For "push" transactions, the payload contains the transmitted patient data, including patient demographic information and identifiers. For data requests in "pull" transactions, the payload contains any patient demographic information or identifiers used to specify the patient for whom data are requested. For data responses in "pull" transaction, the payload contains the transmitted patient data.

Note that the HIE Payload section is the only part of the message that may contain protected health information. This section may optionally be encrypted using the receiving entity's public key or the receiving provider's public key.

1.2.2. Content Security

Message Signature: XML Signature standard (per WS-I Security Profile 1.1)

Canonicalization method: Exclusive Canonicalization (http://www.w3.org/2001/10/xml-exc-c14n#).

Signature method: RSA signing and verification (http://www.w3.org/2000/09/xmldsig#rsa-sha1)

Message Encryption: XML Encryption Standard (per WS-I Security Profile 1.1)

Encryption method: 128-bit AES (http://www.w3.org/2001/04/xmlenc#aes128-cbc)

1.3. Critical Functions of Solution

The responding Bidder may propose variations to the specifications described above as long as the Bidder's specifications are functionally equivalent. The critical functions that must be met by the vendor's proposed solution are listed in Table 1.2

Table 1.2 Critical functions of the solution for the Messaging Framework

No.	CRITICAL FUNCTIONS
MF-1	SOAP messages transmitted over HTTP with Transport Layer Security (TLS). The framework will conform to the WS-I Basic Profile 2.03 and the WS-I Security Profile 1.14. These profiles use the web-services standards specified in the above table, but prescribe further constraints to improve interoperability
MF-2	Support the following transactions and message exchange pattern (MEP)s: • Push: Deliver Laboratory Test Result to Ordering Provider and Copied Provider(s) and/or Send Ambulatory Patient Summary from One Provider to Another • Request/reply ("pull"): Request and receive information from the ELPD and ILPD and request and receive an Ambulatory Patient Summary • Publish-Subscribe: Register subscriber interest with publisher of clinical data on a specific patient. Publisher will send updates ("push") as they are available without further action on the part of the subscriber
MF-3	Use security protocols equally robust to those listed in the table above
MF-4	Have the ability to sign message contents to ensure non-repudiation of source
MF-5	Include the option to encrypt message contents for viewing by intended recipient only

[3] See http://www.ws-i.org/Profiles/BasicProfile-2_0(WGD).html for detailed technical specifications.

[4] See http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html for detailed technical specifications.

No.	CRITICAL FUNCTIONS
MF-6	Include sufficient information and security features to allow intermediate nodes to route message contents to the final intended recipient without compromising security

2. Authorization Framework

The Authorization Framework is a set of specifications that defines a trust model for exchanging protected health information using the Messaging Framework. The Authorization Framework also describes the security model for interacting with the ILPD and ELPD via a web-services interface.

2.1. Functional Requirements

The authorization framework consists of two parts: (1) a *Certificate Authority* that certifies Entities and Providers as participants in good standing in the Cal eConnect infrastructure, and (2) a set of *authorization artifacts* that enable sending Entities to formally attest to the source of messages in a manner that receiving Entities or receiving Providers can validate.

2.1.1. Certificate Authority

Cal eConnect (directly or through third parties) will serve as the Certificate Authority (CA) for all Entities participating in the Cal eConnect Infrastructure, as well as for those Providers who are licensed professionals (physicians, pharmacists, etc.). Specifically, Cal eConnect will issue digital certificates to the Entities registered in the ELPD and the licensed medical professionals registered in the ILPD. Un-licensed professionals and other types of Providers will be issued digital certificates by the Entities with which they are associated – See Section 6.1. Because these Entities are themselves certified by Cal eConnect, a chain of trust will exist between the digital certificates of all Providers and Cal eConnect.

The CA will need to interact with the technical infrastructure in several ways:

1. The CA will create and sign digital certificates for qualified Entities and Providers and add these certificates to the ELPD and ILPD, respectively.
2. The CA will deliver the key pairs for digital certificates to Providers and Entities in a secure manner, for example through “out of band” communications, as needed.
3. When digital certificates expire, the CA will create new certificates and add these to the ELPD and ILPD.
4. The CA will revoke existing certificates and add new certificates to the ELPD and ILPD when the contents of certificates need to be updated (e.g., the legal name of the Entity has changed)
5. The CA will revoke existing certificates in the ELPD and ILPD if entities are judged to have violated the terms of participation in the Cal eConnect Infrastructure (following a formal adjudication process).
6. The CA will periodically publish the list of revoked certificates (revocation list) to all participants in the Cal eConnect Infrastructure.

The ELPD and ILPD (described in Section 3 and Section 4, respectively) will need to support these operations in a highly secure manner. The digital certificates stored in the ELPD and ILPD will form the foundation of the trust model for the Cal eConnect Infrastructure.

2.1.2. Authorization Artifacts

The authorization artifacts must express in a trusted manner the following claims about the message in which they are included:

1. <u>The identity of the sending Entity</u>. This claim is expressed through two artifacts:

   (A) A *digital certificate* whose subject is the sending Entity and which is signed by the CA. The digital certificate includes attributes of the sending Entity sufficient to unambiguously identify it, as well as the sending Entity's PKI public key.

   (B) The *digital signature* of the sending Entity, such that message recipients may validate the signature using the Entity's public key. The purpose of the digital signature is to authenticate the sending entity and to validate the integrity of the transmitted message. The digital signature is specifically *not* intended as any form of medical attestation of the health information payload. Such attestation, if required, should be sent as part of the payload itself.

2. <u>The identity of the sending Provider</u>. This claim is expressed through two artifacts:

   (A) A *digital certificate* whose subject is the sending Provider and which is signed either by the Cal eConnect CA (for licensed professionals only) or by the sending Entity (for licensed professionals and other types of Providers). The digital certificate includes attributes of the sending Provider sufficient to unambiguously identify it, as well as the sending Provider's public key.

   (B) An *authentication assertion* that indicates the Provider sending the message was properly authenticated, as well as the manner and time of authentication. The authentication assertion is signed by the sending entity, such that message recipients may validate the signature using the Entity's public key. By signing this assertion, the sending entity is effectively attesting to the proper authentication of the sending provider.

3. <u>The sending Provider's stated reason for requesting PHI (required for the "Pull" and "Publish/Subscribe" message patterns only)</u>. This claim is expressed through an authorization assertion that contains at least two pieces of information:

   (A) The professional role of the requesting provider (e.g., physician, nurse, pharmacist, administrator)

   (B) The "reason for use" of the PHI that the sending provider is requesting (e.g., "patient treatment," "public health," "research," "payment").

   The authorization assertion may be signed by the sending Entity or the sending Provider, such that message recipients may validate the signature using the Entity's or Provider's public key (respectively). By signing this assertion, the sending Entity or Provider is attesting to the indicated role and reason for use as justification for the disclosure of PHI.

Table 2.1 represents the requirements for each of these artifacts depending on the kind of message transmitted via the messaging framework. Note that the matrix distinguishes between messages relating to PHI and messages related to information stored in the Entity Level Provider Directory or Individual Level Provider Directory. See Section 1.1.1 and 1.1.2 for more information about the sequence of messaging that takes place during push and pull transactions.

In addition to the authorization artifacts listed in Table 2.1, future uses of the Messaging Framework may also require a "Consent Assertion." A Consent Assertion will enable a Provider who is requesting PHI from another Provider to assert that the subject patient has specifically consented to this disclosure of her information. Although such consent is implicit in the Authorization Assertion already included in Table 2.1, disclosures of PHI that are not subject to HIPAA exclusions (e.g., research uses) may require explicit assertion of the patient's consent.

Table 2.1 Matrix of authorization artifacts required, by message pattern and message type

			Authorization Artifact ("R" = Required)				
Message Pattern	**Type of Data**	**Type of Message**	**Digital Certificate (Sending Entity)**	**Digital Signature (Sending Entity)**	**Digital Certificate (Sending Provider)**	**Authentication Assertion (Sending Provider)**	**Authorization Assertion (Provider Requesting PHI)**
Push	PHI	Send PHI	R	R	R	R	
		Ack to send	R	R	R	R	
	Core Services Records	Write ELPD/ ILPD Records	R	R	R	R	
		Ack to write	R	R			
Pull + Publish/ Subscribe	PHI	Request PHI	R	R	R	R	R
		Ack to request	R	R	R	R	
		Deliver PHI	R	R	R	R	
		Ack to delivery	R	R	R	R	
	Core Services Records	Request ELPD Records	R	R			
		Request ILPD Records	R	R	R	R	
		Ack to request					
		Deliver ELPD/ ILPD Records					

Note: "ELPD" = Entity Level Provider Directory; "ILPD" = Individual Level Provider Directory; "R" = Required.

2.2. Technical Specifications

The authorization artifacts will be represented as data structures consistent with WS-I Security Profile 1.12. The specific standards for each type of artifact are listed in Table 2.2, with details available in the documentation of the WS-I Security Profile.

Table 2.2 Standards specifications for authorization artifacts

Authorization Artifact	**Specification**	**Version**	**Comments**
Digital Certificate (Sending Entity)	X.509 Token Profile	1.0	Signed by certificate authority
Digital Signature (Sending Entity)	XML Signature	1.0	Signature of sending entity via Exclusive Canonicalization and RSA-SHA-1 encryption (See Section 3.4 in NHIN Authorization Framework v1.0[v])
Digital Certificate (Sending Provider)	X.509 Token Profile	1.0	Signed by CA or Entity (depending on type of Provider)
Authentication Assertion (Sending Provider)	SAML Token Profile	1.1	Signed by sending entity per the specifications in this table
Authorization Assertion (Provider Requesting PHI)	SAML Token Profile	1.1	Signed by sending entity per the specifications in this table

2.2.1. Contents of Authorization Artifacts

To conform to the Authorization Framework, the authorization artifacts appearing in messages will need to contain the specific fields indicated in Table 2.3.

Table 2.3. Fields to be included in authorization artifacts, by artifact type

Artifact Type	Field	Value Set/Comments
Digital Certificate (Entity)	(See Section 3.2.1 for contents of Entity digital certificates)	
Digital Signature (Entity)	XML element formatted per the Digital Signature specification in Table 2.2	Digital signature of the sending entity over the entire SOAP Body contents (including the Service Parameters). See Section 1.2.1 for specification of SOAP Body contents.
Digital Certificate (Provider)	(See Section 6.2.1.1 for contents of Provider digital certificates)	Subject Name must match the value of "FROM" address in the transmitted message
Authentication Assertion (Provider)	Unique ID of sending provider	Must match the Subject Name in the Provider Certificate, if one was sent; otherwise, must represent a unique Provider within the sending Entity's name space
	Authentication method	See Section 3.3 in NHIN Authorization Framework v1.0[v]
	Authentication time	See Section 3.3 in NHIN Authorization Framework v1.0[v]
Authorization Assertion (Provider)	Unique ID of sending provider	Must match the Subject Name in the Provider Certificate, if one was sent; otherwise, must represent a unique Provider within the sending Entity's name space
	Role of sending provider	SNOMED-CT code
	"Purpose of use" for PHI	See "Purpose of use" vocabulary in NHIN Authorization Framework v1.0[v]

2.3. Critical Functions of Solution

The responding Bidder may propose variations to the specifications described above as long as the Bidder's specifications are functionally equivalent. The critical functions that must be met by the vendor's proposed solution are listed in Table 2.4.

Table 2.4. Critical functions of the solution for the Authorization Framework

No.	CRITICAL FUNCTIONS
AF-1	Identity management of Entities and licensed Providers should be based on X.509 class-3 digital certificates
AF-2	Requires the inclusion of the sending Entity's digital certificate and digital signature in all transmissions
AF-3	Allows the sending Entity to authenticate the sending Provider using a variety of 1-factor or 2-factor methods, as determined by the sending Entity

3. Entity Level Provider Directory

The Entity Level Provider Directory (ELPD) is a secure repository of information about entities and nodes that participate in the Cal eConnect Infrastructure. The repository provides a web services API for both the reading and writing of this information. It also provides a web browser interface for reviewing information related to Entities.

The sections below describe the functional, technical, and performance requirements of the service.

3.1. Functional Requirements

The goal of the ELPD is to enable participants in the Cal eConnect Architecture to discover information about the entities that are their potential counterparties in HIE transactions, including the appropriate addressing, protocol, and trust information for these entities. Mappings between the ELPD and Individual Level Provider Directory (ILPD) enable participants to discover the individual providers that are associated with the entities and to retrieve the appropriate trust artifacts and other data needed to exchange health information with these providers.

A variety of transport mechanisms and trust infrastructures are envisioned for HIE in California, including the Direct Project, NwHIN Exchange, and the mechanisms described in this document. The design of the ELPD is intended to provide directory services to support all of these transport mechanisms and trust infrastructures, if possible.

Functionally, the ELPD securely maintains a hierarchical representation of the entities and nodes that participate in the Cal eConnect Infrastructure, as well as the trust artifacts for these entities and nodes (specifically, their digital certificates). The ELPD supports read and write access to these objects via a web services API and web browser interface.

The ELPD is intended to securely maintain information about a variety of Entity types, including those listed in Table 3.1

Table 3.1. The types of Entities that shall be represented in the ELPD

Priority	Type of Entity	Estimated Number in CA
1	HIEs, HIOs, HISPs	20
	Hospitals / IDNs	360
	Clinics	TBD
	Physician offices / Groups	TBD
	State and Federal health agencies	TBD
	Clinical laboratories	TBD
	Pharmacies / Pharmacy networks	TBD
	Imaging centers	TBD
	Health plans (including Medi-Cal, Medicare)	30
	Health centers and FQHCs	900
2	Transaction intermediaries	TBD
	Nursing homes	TBD
	Home health agencies	TBD
	Professional organizations	TBD
3	Rehabilitation facilities	TBD
	Mental health facilities	TBD
	Long term care facilities	TBD
	Hospice	TBD
4	HME/DME providers	TBD
	Other Business Associates	TBD
5	Personal health records/repositories	TBD

3.1.1. Conceptual Data Model

The conceptual data model of the ELPD is depicted in Figure 3.1. The model denotes a hierarchical organization of entities, sub-entities, and nodes. Sub-entities are parts of entities, such as organizational sub-components, geographically distinct facilities, etc. The purpose of sub-entities is to divide entities into distinct units that may be associated with different sets of providers and may have different methods for sending and receiving HIE transactions.

For example, a national hospital chain may have sub-entities denoting states, cities, or individual hospital facilities, all respectively nested within the ELPD hierarchy. Providers who work for the hospital chain may be associated with one or more individual hospitals, which themselves may have different technologies in place for sending and receiving HIE transactions. In order to effectively communicate with a specific provider, it is important to specify the organizational context in which the communication is taking place (i.e., to which or from which hospital) and the technical addressing and formatting details needed to conduct an electronic HIE transaction with that hospital. This information is stored in the ELPD.

Figure 3.1. General Structure of Objects in ELPD

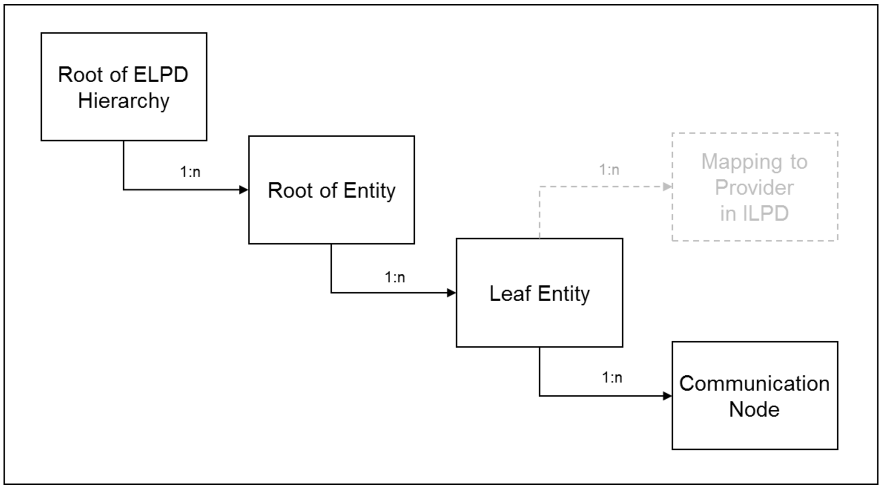
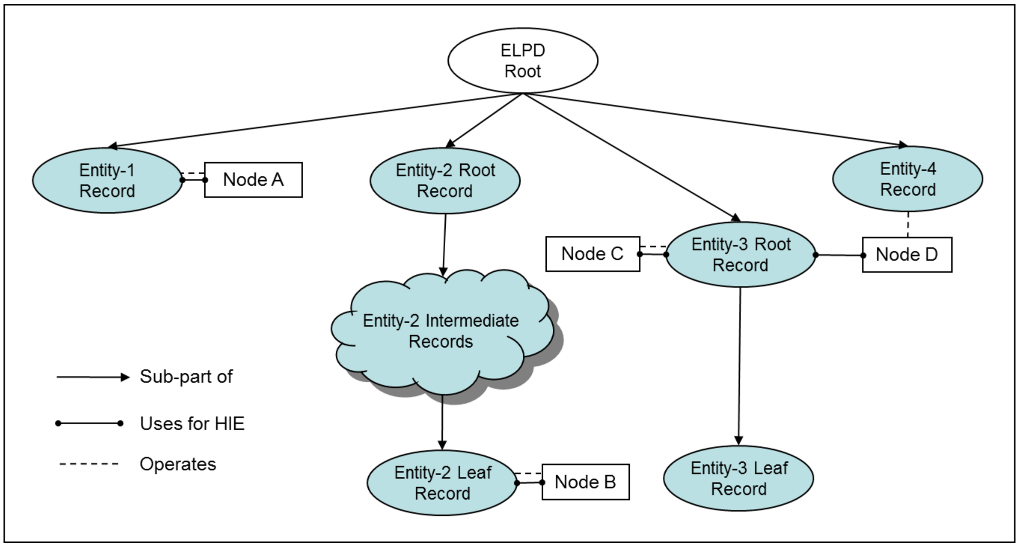


Figure 3.2 shows an example of several entities and nodes as they are organized in the ELPD. Note that there are actually two types of relationships between Entities and Nodes: "Uses for HIE" and "Operates." Although in most cases, Entities operate the nodes that they use for HIE transactions, this is not necessarily the case. Specifically, an entity may use a node operated by a third party, such as a local HIO, an NwHIN Gateway provider, or a commercial HIE provider, to conduct certain HIE transactions.

Figure 3.2 also shows that an Entity may be associated with multiple Nodes, with each Node supporting different types of transactions or supporting the same transactions using different protocols and standards. Lastly, Nodes may be associated with Entities at any level of the Entity hierarchy, and the functionalities of Nodes are inherited by Entities at lower levels of the hierarchy. For example, Entity-3 in Figure 3.2 inherits the capabilities of Node C. This inheritance behavior within the ELPD allows organizations to provide HIE services using a centralized technology (Node) that serves all of the organization's sub-parts. Alternatively, organizations may use separate technologies (Nodes) for HIE services at each of their subsidiaries, in which case different Nodes would be associated with each leaf Entity.

Figure 3.2 Example of Entities and Nodes in ELPD



The ELPD will be used in conjunction with the ILDP (see Section 6) in most cases, so it is useful to review the relationship between the two resources to fully understand the intent and requirements of the ELPD. Figure 3.3 shows the mapping relationship between Entities in the ELPD and Providers in the ILPD. The diagram shows the example of a single Provider who is associated with three different Entities and conducts HIE transactions differently in the context of each entity.

Note that Operationally, the mapping between the ELPD and ILPD shall be used to determine (1) the set of Providers who are associated with a known Entity and can, therefore, receive or send HIE transactions in the context of that entity, and (2) the set of Entities with which a particular Provider is associated and the Nodes, transactions, and interoperability protocols that those Entities make available to exchange information with that Provider. Notably, the ILPD contains no information about the specific transactions that can be conducted with the Providers listed therein, nor the network nodes, internet addresses, and interoperability protocols that may be used to exchange information with the Providers. Rather, all of that information is specific to and the responsibility of the Entities with which the Providers are associated, and therefore represented in the ELPD.

For example, Figure 3.4 depicts a specific situation in which a single Provider, Dr. Hill, is associated with three different entities. Each entity uses different I.T. resources (“Nodes”) to conduct HIE transactions, and the mapping between Dr. Hill and each Entity determines which Node should be used to send health information to Dr. Hill in the context of that Entity. Specifically, when sending health information to Dr. Hill at the community clinic, the appropriate Node to receive the information is “EHR-1.” Alternatively, when sending information to Dr. Hill at the hospital, the HIE transaction should be performed with the “H.I.S.” node. Lastly, when communicating with Dr. Hill in the context of his Internal Medicine practice, the communication should take place with either his local EHR, “EHR-2”, or with a gateway operated by the HIO in which Dr. Hill’s practice participates. The choice of Node in this latter case will depend on the type of transaction to be conducted, since “EHR-2” and “HIE Gateway” may support different transactions. In all cases, however, the transactions, protocols, and addresses to be used when communicating with Dr. Hill at each of his associated entities is specified within the Node records corresponding to those Entities within the ELPD.

Figure 3.3. Schematic for Mapping between Objects in the ELPD and ILPD

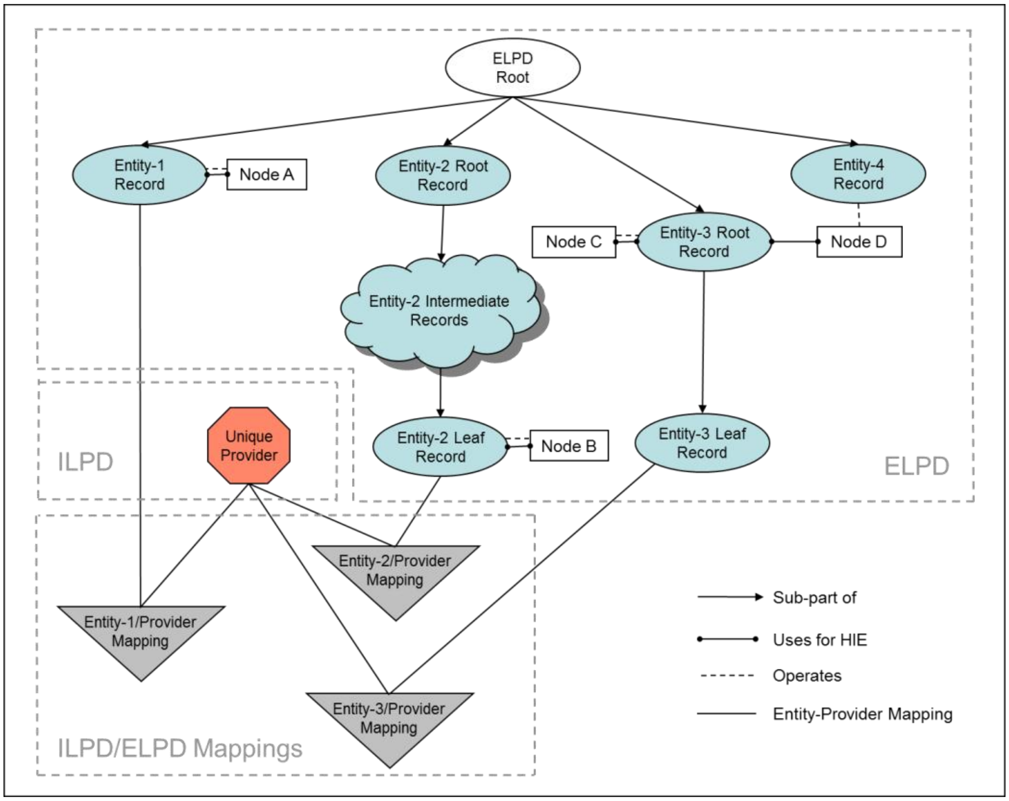
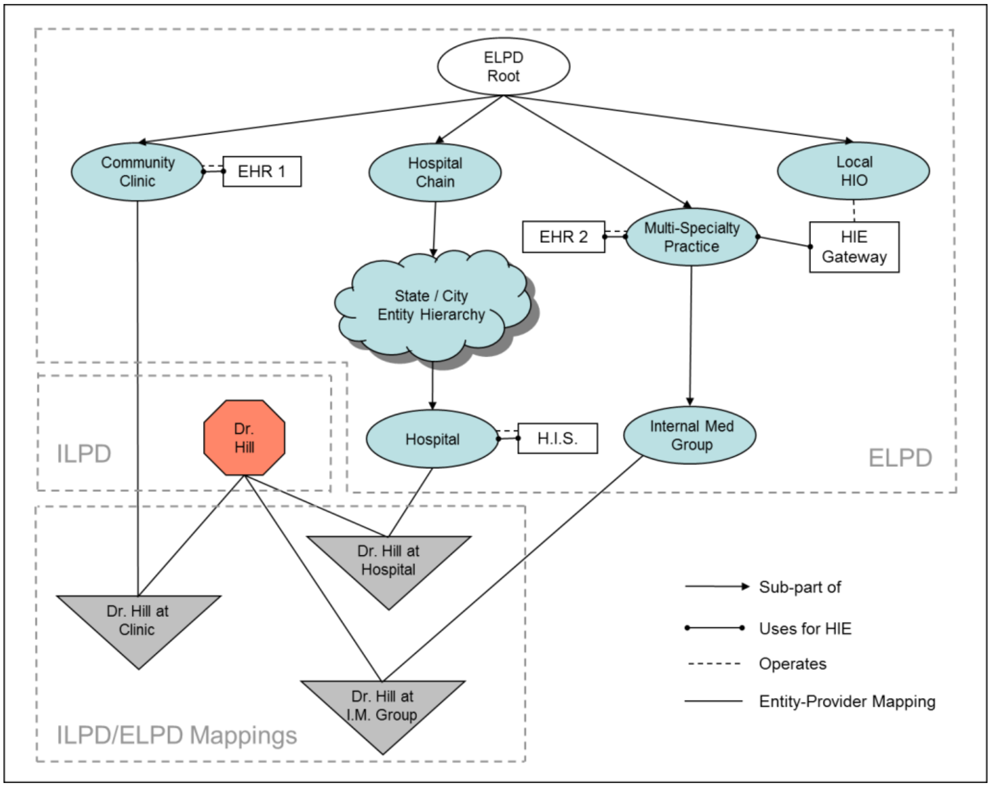


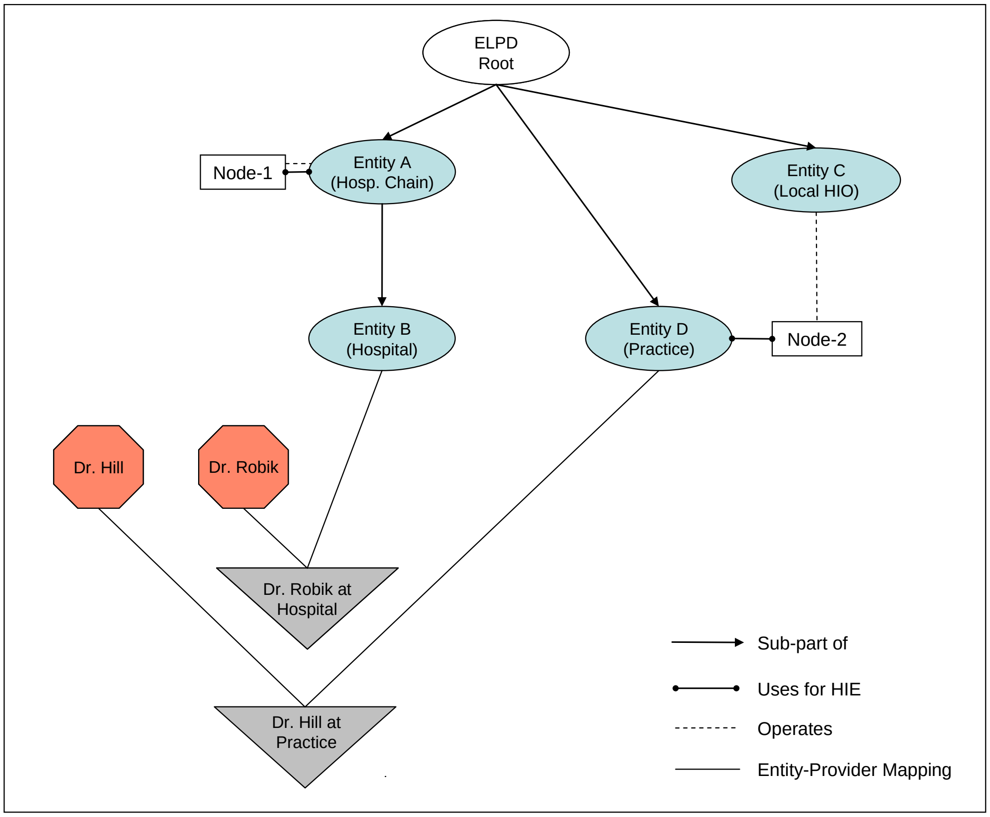
Figure 3.4 Example of Mapping between Objects in the ELPD and ILPD



3.1.2. Inheritance of Nodes, Transactions, and Interoperability Protocols

A feature of the ELPD data model is that Entities may use Nodes that are operated by other Entities. Figure 3.5 illustrates this feature by showing two Entities (Entity B and Entity D) that use Nodes operated by other Entities (Node-1 and Node-2, respectively).

Figure 3.5 Examples of Entities inheriting other Entities' Nodes



In certain cases, a leaf Entity may "inherit" the functionality of a Node that is operated by its parent or ancestor Entity. For example, Entity B (a hospital) "inherits" the functionality of Node-1, which is operated by its parent Entity, Entity A. The hospital's inheritance of Node-1's interoperability capabilities implies that the Providers associated with the hospital can receive messages addressed to them that are received by Node-1 and/or can send messages to other Providers via Node-1. Specifically, the Providers may use the transactions, addresses, and interoperability protocols that are supported by Node-1 to exchange health information with other Providers. The manner in which messages pass between Node-1 and the Providers at Entity B need not conform to the Messaging and Authorization Frameworks of the Cal eConnect Infrastructure, as long as Node-1 supports these frameworks for communications with "external" Entities.

In other cases, an Entity may use a Node operated by an unrelated Entity that serves as an interoperability gateway or routing service (such as an HIO, HISP, or NwHIN Exchange Node). For example, Entity D (a physician practice) uses Node-2, which is operated by a Local HIO, Entity C. The practice's "inheritance" of Node-2's interoperability capabilities implies that the Providers associated with the practice can receive messages addressed to them that are received by Node-2 and/or can send messages to other Providers via Node-2. Specifically, the Providers may use the transactions, addresses, and interoperability protocols that are supported by Node-2 to exchange health information with other Providers. Again, the manner in which messages pass between Node-2 and the Providers at Entity D need not conform to the Messaging and Authorization Frameworks of the Cal eConnect Infrastructure, as long as Node-2 supports these frameworks for communications with "external" Entities.

These inheritance features are useful for allowing multiple Entities to share a Node without requiring the ELPD to redundantly store and maintain the interoperability capabilities of that Node within each of those Entities' records. However, the feature also introduces a potential complication, because an Entity that uses a Node operated by another Entity may not necessarily support all of the interoperability capabilities of that Node (i.e., all of the transactions and interoperability protocols). For example, in Figure 3.5, Node-2 may support the full range of transactions and interoperability protocols defined for the Cal eConnect Infrastructure (see Section 4), but Entity D may be incapable of receiving electronic patient summaries or incapable of responding to electronic requests for patient summaries because its local EHR cannot support those specific functions (whereas other Entities that use Node-2 may be able to support those functions). Therefore, it is necessary to represent for each Entity any interoperability capabilities of an inherited Node that the Entity does not, in fact, support, i.e. "Entity transaction exceptions." This information is critical to alert users of the ELPD that they cannot transmit messages to Providers associated with that Entity using those non-supported transactions and/or interoperability specifications.

The representation of Entity transaction exceptions is described Section 3.2.1. Note that an Entity by default will support *all* of the transactions and interoperability protocols of the Nodes that it inherits from a parent or ancestor (and any it does not support must be explicitly listed), whereas an Entity by default will support *none* of the transactions and interoperability protocols from a Node operated by a hierarchically unrelated entity (and any it does support must be explicitly listed). For example, in Figure 3.5, Dr. Robik can communicate using any of the transactions and interoperability protocols provided by Node-1 with the exception of those explicitly listed as exceptions for Entity A, whereas Dr. Hill can communicate using only those transactions and interoperability protocols provided by Node-2 that have been explicitly listed as supported by Entity D.

3.1.3. Support for the Trust Models of the Direct Project and NwHIN Exchange

The ELPD, ILPD, and mappings between them will support HIE transactions performed per the messaging and authorization specifications of the Direct Project and NwHIN Exchange. The messaging specification and trust models of the Direct Project and NwHIN Exchange are distinct from those specified in this document for California's infrastructure. However, it is anticipated that the ELPD, ILPD, and the mappings between them may be used by other states for their own HIE infrastructures or for enabling health information exchange between entities in those states and entities in California. Therefore, given the potential use of the Direct Project and NwHIN Exchange in California and other states, the design and operation of the directory components of the Cal eConnect infrastructure should support these alternative messaging and authorization specifications.

Figure 3.6 illustrates the use of the ELPD and ILPD to support the Direct Project trust model. In this model, end-users are assigned "Direct Addresses" by a HISP, which include the HISP's domain name and must be incorporated into the end users' digital certificates. Therefore, a digital certificate specific to the association between the provider (Dr. Hill, in the example) and the HISP Entity is required. It is envisioned that this certificate will be stored in the mapping record between the Provider and the Entity, rather than in the ILPD, since it will be specific to the HISP.

Figure 3.6 Use of the ELPD and ILPD to support the Direct Project trust model

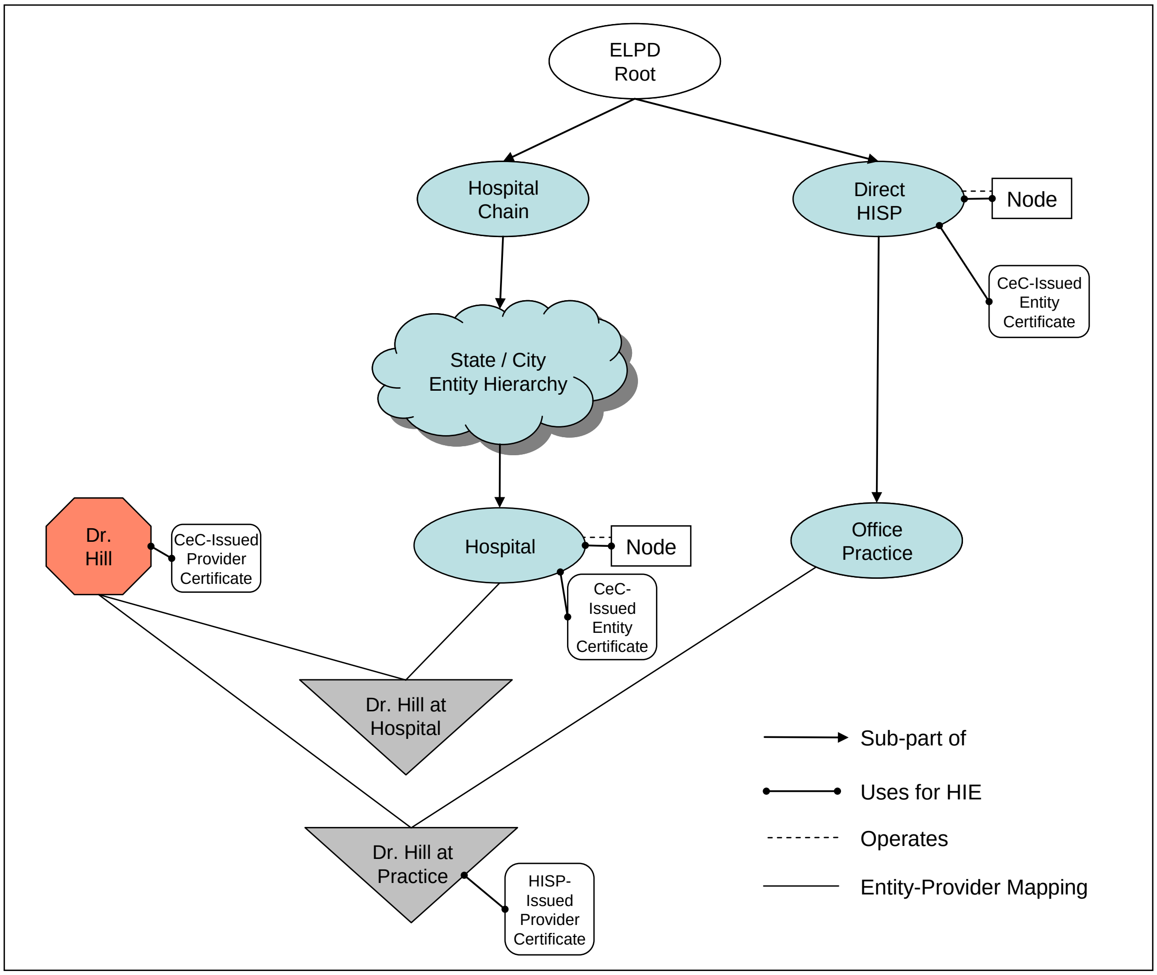
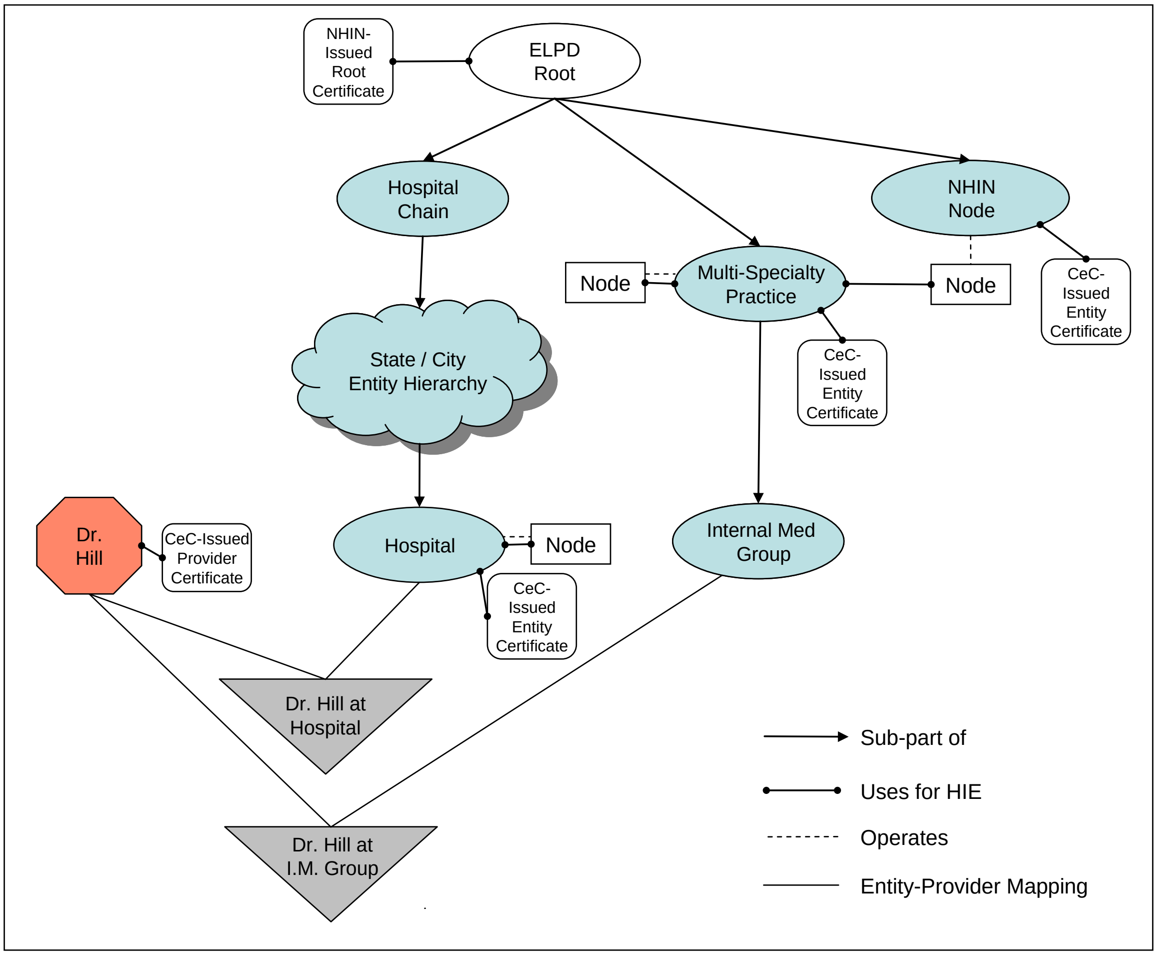


Figure 3.7 illustrates the use of the ELPD and ILPD to support the NwHIN Exchange trust model. In this model, an “NwHIN Node” (gateway) must have a digital certificate for purposes of signing various security assertions and signing/encrypting messages in TLS transactions. This certificate must be linked, through a chain of trust, with the NwHIN Root Certificate Authority. Therefore, Cal eConnect’s own digital certificate, which is used to issue the NwHIN Node’s certificate, must be signed by the NwHIN Root Certificate Authority. At the same time, the NwHIN Exchange trust model does not require the use of digital certificates to sign or encrypt message content in a manner specific to the Provider or Entity involved in the communication (attestation of the Provider’s and Entities identities, authentication, and authorization is delegated to the NwHIN Node). Therefore, the digital certificates already stored in the ELPD and ILPD for Entities and Providers will suffice to support NwHIN Exchange transactions.

Figure 3.7 Use of the ELPD and ILPD to support the NwHIN Exchange trust model



3.1.4. Read Access via API

Read access to the ELPD shall be broadly available from any node that is, itself, registered in the ELPD. The retrieval of information from the ELPD is intended to meet the following needs of participants in the HIE infrastructure:

1. Determination of whether an organization is registered in the ELPD as a certified entity approved to participate in the HIE infrastructure. This query shall enable HIE participants to discover an organization's ELPD record(s) (and access the information therein) when the entity's unique ID is not known. Navigation and search of the ELPD shall leverage the hierarchical structure.

2. Look up of the Individual Providers associated with an entity. This query shall enable participants to discover the Individual Providers for an entity when the entity's unique ID is known. The lookup may be confined to those Providers associated with a specific Entity record or expanded to include all Providers associated with an Entity record or any descendant record in the hierarchical structure.

3. Determine whether a node is approved to participate in the HIE infrastructure. This query will enable HIE participants to determine whether a URL address corresponds to a node that appears in the ELPD.

4. Access the list of digital certificates for entities and nodes that have been revoked by the certificate authority (“revocation list”).
5. Access an ELPD Entity by its unique ID to determine whether the Entity is currently in good standing and has an active Digital Certificate.

To meet these needs, the ELPD will provide the following web-service functions:

Table 3.2 API functions for read access to ELPD

Function	Input Parameter(s)	Return Parameter(s)
Search for entity by name and related descriptors (including Entity type, geographical location, etc.)	Text Search Term(s)	Unique IDs, legal names and DBA names of matching entities
Retrieve Entity record by unique ID	Unique ID of entity within ELPD	Record of the specified Entity, including its digital certificate and Unique IDs of the Entity’s Node record(s)
Retrieve Entity record and All related Node records by Entity’s unique ID	Unique ID of entity within ELPD	Record of the specified Entity, including its digital certificate, and records of all Nodes related to the Entity, including the transactions, addresses, and interoperability protocols supported by the Node that are also supported by the Entity (per Section 3.1.2) (will require call by ELPD to the Services Registry),
Retrieve “header” information for Individual Providers associated with the Entity	Unique ID of entity within ELPD + search/filter criteria (including Provider Type, Provider name, Provider NPI, local vs. hierarchical search, etc.)	Unique IDs, full names, specialties, and work locations of matching entries in the ILPD
Retrieve detail information for Individual Provider associated with the Entity	Unique ID of Provider, Unique ID of Entity	Full Provider record + corresponding ILPD/ELPD Mapping record for that Provider in the context of the current Entity

Function	Input Parameter(s)	Return Parameter(s)
Retrieve Node record by Node unique ID	Unique ID of node within ELPD	Record of the specified Node, including its digital certificate and all related information describing the transactions, addresses, and interoperability protocols supported by the node (will require call by ELPD to the Services Registry)
Retrieve Node record by address (URL)	URL	Record of the Node that corresponds to (services) requests made at the designated URL (returns null if the URL does not correspond to a Node registered in the ELPD)
Retrieve revocation list for entities	Date of last revocation list retrieval (may be NULL)	All revocation list(s) since date of last retrieval (or, if no date provided, all revocation lists)
Retrieve revocation list for nodes	Date of last revocation list retrieval (may be NULL)	All revocation list(s) since date of last retrieval (or, if no date provided, all revocation lists)
Retrieve status of an Entity by the Entity's unique ID	Unique ID of entity within ELPD	Record of Entity's status as a participant in good standing in the Digital Architecture, as well as a copy of the Entity's currently active digital certificate (or an indication that the Entity has no currently active certificate)
Retrieve status of a Node by the Node's Unique ID	Unique ID of Node within ELPD	Record of Node's status as a participant in good standing in the Digital Architecture, as well as a copy of the Node's currently active digital certificate (or an indication that the Node has no currently active certificate)

Function	Input Parameter(s)	Return Parameter(s)
Retrieve status of a digital certificate for an Entity or Node by unique certificate ID	Unique ID of digital certificate	Flag indicating whether the certificate is currently valid.

As specified in Table 2.1, no authorization artifacts are required for requesting information from the ELPD. However, because such requests are made using the Messaging Framework, the requests must originate from a certified node that is, itself, registered in the ELPD.

The data structure and contents of the records for entities and nodes are specified in Section 3.2.1.

Certificate revocation lists (CRLs) will be published at a frequency that is TBD, pending policy decisions.

3.1.5. Read Access via Web Browser

In addition to a web-services API, the ELPD will also support read access from web browsers. This capability will allow Providers to access information in the ILPD directly via the internet for purposes of discovering their counterparties for H.I.E. transactions and determining which transactions and interoperability protocols these counterparties support. Table 3.3 lists the read operations that will be available via web browser.

Table 3.3. Web browser operations for read access to ELPD

Function	Input Parameter(s)	Return Parameter(s)
Search for Entity by name and related descriptors (including Entity type, geographical location,	Text Search Term(s)	Unique IDs, legal names and DBA names of matching entities
Retrieve Entity record by unique ID	Unique ID of entity within ELPD	Data elements within record of the specified entity, including the Unique IDs of the Entity's Node record(s) [including any inherited Nodes]

Function	Input Parameter(s)	Return Parameter(s)
Retrieve Entity record and All related Node records by Entity’s unique ID	Unique ID of entity within ELPD	Record of the specified Entity, including its digital certificate, and records of all Nodes related to the Entity, including the transactions, addresses, and interoperability protocols supported by the Node that are also supported by the Entity (per Section 3.1.2) (will require call by ELPD to the Services Registry),
Retrieve “header” information for Individual Providers associated with the Entity	Unique ID of entity within ELPD + search/filter criteria (including Provider Type, Provider name, Provider NPI, local vs. hierarchical search, etc.)	Unique IDs, full names, specialties, and work locations of matching entries in the ILPD
Retrieve detail information for Individual Provider associated with the Entity	Unique ID of Provider	Public data elements from full Provider record + data elements from corresponding ILPD/ELPD Mapping record for that Provider in the context of the current Entity
Retrieve Node record by Node unique ID	Unique ID of Node within ELPD	Data elements in record of the specified Node, including all related information describing the transactions, addresses, and interoperability protocols supported by the node (will require call by ELPD to the Services Registry)
Retrieve Node record by address (URL)	URL	Data elements in record of the Node that corresponds to (services) requests made at the designated URL (returns null if the URL does not correspond to a Node registered in the ELPD)

Function	Input Parameter(s)	Return Parameter(s)
Retrieve status of an Entity by the Entity's unique ID	Unique ID of entity within ELPD	Entity's status as a participant in good standing in the Digital Architecture, as well as key information from the Entity's currently active digital certificate (such as the signer of the certificate and the date it was issued)
Retrieve status of a Node by the Node's Unique ID	Unique ID of Node within ELPD	Node's status as a participant in good standing in the Digital Architecture, as well as key information from the Node's currently active digital certificate (such as the signer of the certificate and the date it was issued)

Read access to the ELPD via web browser will only be available to Providers registered in the ILPD. One-factor authentication (password) will be sufficient to authenticate Providers seeking read access to the ELPD.

The contracted vendor shall design and implement the user-interface components such that they maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.

3.1.6. Write Access via API

Write access to the ELPD is tightly controlled. The updating of information in the ELPD is intended to meet the following needs of the Cal eConnect infrastructure:

1. Entering and updating ELPD records for Entities that participate in the Cal eConnect infrastructure (including the revocation and/or replacement of the digital certificates for Entities). These operations will be available only to the certificate authority.

2. Entering and updating ELPD records for Nodes that participate in the Cal eConnect infrastructure (including the revocation and/or replacement of the digital certificates for Nodes). These operations will be available only to the certificate authority.

3. Requesting the revocation and/or replacement of a digital certificate for a node that participates in the HIE infrastructure. These requests will be made by Entities to update the nodes that they control. In certain cases and with the proper authorization, such requests may be fulfilled automatically (i.e., without human intervention). For example, if an Entity needs to revoke the digital certificate of a node that has been compromised, the Entity could request that this be effected immediately.

To meet these needs, the ELPD will provide the web-service functions listed in Table 3.4. Note that the functions designated with a "*" will be available only to the certificate authority. The remaining functions will be available only to external users who are associated with the Entity to whom the ELPD records pertain.

Table 3.4. API functions for write access to ELPD

Function	Input Parameter(s)	Return Parameter(s)
Insert new record – Entity (except for digital certificate)	Required data for an Entity (see Section 3.2.1), Unique ID of parent Entity	Acknowledgement (success/fail)
Insert new record – Node (except for digital certificate)	Required data for a Node (see Section 3.2.13.2.1), Unique ID of associated Entity	Acknowledgement (success/fail)
Insert new record – Transaction	Unique ID of Node, Required data for a transaction, including protocol information (see Table 3.9 and Table 3.10)	Acknowledgement (success/fail), Unique ID of Node-Transaction
Update existing record – Entity (except for digital certificate)	Unique ID of Entity, Updated data elements for the Entity	Acknowledgement (success/fail)
Update existing record – Node (except for digital certificate)	Unique ID of Node, Updated data elements for the Node	Acknowledgement (success/fail)
Update existing record – Transaction	Unique ID of Node, Unique ID of Node-Transaction, Updated data elements for transaction, including protocol information (see Table 3.9 and Table 3.10)	Acknowledgement (success/fail)
Activate/Inactivate Inherited Transaction	Unique ID of Entity, Unique ID of inherited Node, Unique ID of inherited Node-Transaction, Desired State (active/inactive)	Acknowledgement (success/fail)

Function	Input Parameter(s)	Return Parameter(s)
Activate/Inactivate Inherited Protocol/Address	Unique ID of Entity, Unique ID of inherited Node, Unique ID of inherited Node-Transaction, Unique ID of inherited Protocol/Address, Desired State (active/inactive)	Acknowledgement (success/fail)
*Delete existing record - Entity	Unique ID of Entity (the associated digital certificate must first be revoked; automatically deletes all descendant Entities)	Acknowledgement (success/fail)
*Delete existing record - Node	Unique ID of Node (the associated digital certificate must first be revoked)	Acknowledgement (success/fail)
Delete existing record – Transaction	Unique ID of Node, Unique ID of Node-Transaction	Acknowledgement (success/fail)
*Create new certificate – Entity	Required contents of the digital certificate – See Section 3.2.1, Unique ID of Entity to which certificate will be associated	Acknowledgement (success/fail/review pending) New certificate will be added to the Entity record; Private key will be provided to Entity out-of-band in a manner TBD.
*Replace existing certificate – Entity	Unique ID of Entity, Serial # of certificate to revoke, Required contents of the new digital certificate – See Section 3.2.1	Acknowledgement (success/fail/review pending) New certificate will be added to the Entity record; Private key will be provided to Entity out-of-band in a manner TBD.
*Revoke existing certificate - Entity	Unique ID of Entity, Serial # of certificate to revoke	Acknowledgement (success/fail/review pending)
Request revocation of existing certificate - Entity (Request to revoke Entity certificate; may only be made by the Entity that operates the Node)	Unique ID of Entity, Serial # of certificate to revoke	Acknowledgement (success/fail/review pending)

Function	Input Parameter(s)	Return Parameter(s)
Request replacement of existing certificate – Entity (Request to revoke and replace an Entity certificate; may only be made by the Entity that operates the node)	Unique ID of Entity, Serial # of certificate to revoke, Requested contents of the new digital certificate – See Section 3.2.1	Acknowledgement (success/fail/review pending) Copy of created certificate if success; private key will be provided to Entity out-of-band in a manner TBD.
*Create new certificate – Node	Contents of the digital certificate – See Section 3.2.1	Acknowledgement (success/fail/review pending) New certificate will be added to the Node record; Private key will be provided out-of-band in a manner TBD.
*Replace existing certificate – Node	Unique ID of Node, Serial # of certificate to revoke, Contents of the new digital certificate – See Section 3.2.1	Acknowledgement (success/fail/review pending) New certificate will be added to the Node record; Private key will be provided out-of-band in a manner TBD.
*Revoke existing certificate - Node	Unique ID of Node, Serial # of certificate to revoke	Acknowledgement (success/fail/review pending)
Request revocation of existing certificate - Node (Request to revoke Node certificate; may only be made by the Entity that operates the Node)	Unique ID of node, Serial # of certificate to revoke	Acknowledgement (success/fail/review pending)
Request replacement of existing certificate – Node (Request to revoke and replace a Node certificate; may only be made by the Entity that operates the node)	Unique ID of node, Serial # of certificate to revoke, Requested contents of the new digital certificate – See Section 3.2.1	Acknowledgement (success/fail/review pending) Copy of created certificate if success; private key will be provided to Entity out-of-band in a manner TBD.

The data structure and contents of the digital certificates for entities and nodes are specified in Section 3.2.1.

As specified in Table 2.1, a number of authorization artifacts are required to update information in the ELPD. In addition, all such updates and requests for updates will be rigorously logged by the ELPD.

3.1.7. Write Access via Web Browser

In addition to a web-services API, the ELPD will also support write access from web browsers. Access to operations designated with a “*” will be confined to authorized staff of Cal eConnect and/or its contracted certificate authority, and additional security measures will be taken to prevent unauthorized use of these operations via the public internet (e.g., via IP address filtering). The remaining operations will be available only to external users who are associated with the Entity to whom the ELPD records pertain and who have been authenticated via a two-factor method. Table 3.5 lists the write operations that will be available via web browser.

Table 3.5. Web browser operations for write access to ELPD

Function	Input Parameter(s)	Return Parameter(s)
Insert new record – Entity (except for digital certificate)	Required data for an Entity (see Section 3.2.1), Unique ID of parent Entity	Acknowledgement (success/fail)
Insert new record – Node (except for digital certificate)	Required data for a Node (see Section 3.2.1), Unique ID of associated Entity	Acknowledgement (success/fail)
Insert new record – Transaction	Unique ID of Node, Required data for a transaction, including protocol information (see Table 3.9 and Table 3.10)	Acknowledgement (success/fail), Unique ID of Node-Transaction
Update existing record – Entity (except for digital certificate)	Unique ID of Entity, Updated data elements for the Entity	Acknowledgement (success/fail)
Update existing record – Node (except for digital certificate)	Unique ID of Node, Updated data elements for the Node	Acknowledgement (success/fail)
Update existing record – Transaction	Unique ID of Node, Unique ID of Node-Transaction Updated data elements for transaction, including protocol information (see Table 3.9 and Table 3.10)	Acknowledgement (success/fail)
Activate/Inactivate Inherited Transaction	Unique ID of Entity, Unique ID of inherited Node, Unique ID of inherited Node-Transaction, Desired State (active/inactive)	Acknowledgement (success/fail)

Function	Input Parameter(s)	Return Parameter(s)
Activate/Inactivate Inherited Protocol/Address	Unique ID of Entity, Unique ID of inherited Node, Unique ID of inherited Node-Transaction, Unique ID of inherited Protocol/Address, Desired State (active/inactive)	Acknowledgement (success/fail)
*Delete existing record - Entity	Unique ID of Entity (the associated digital certificate must first be revoked; automatically deletes all descendant Entities)	Acknowledgement (success/fail)
*Delete existing record - Node	Unique ID of Node (the associated digital certificate must first be revoked)	Acknowledgement (success/fail)
Delete existing record – Transaction	Unique ID of Node, Unique ID of Node-Transaction	Acknowledgement (success/fail)
*Create new certificate – Entity	Required contents of the digital certificate – See Section 3.2.1, Unique ID of Entity to which certificate will be associated	Acknowledgement (success/fail/review pending) New certificate will be added to the Entity record; Private key will be provided to Entity out-of-band in a manner TBD.
*Replace existing certificate – Entity	Unique ID of Entity, Serial # of certificate to revoke, Required contents of the new digital certificate – See Section 3.2.1	Acknowledgement (success/fail/review pending) New certificate will be added to the Entity record; Private key will be provided to Entity out-of-band in a manner TBD.
*Revoke existing certificate - Entity	Unique ID of Entity, Serial # of certificate to revoke	Acknowledgement (success/fail/review pending)
Request revocation of existing certificate - Entity (Request to revoke Entity certificate; may only be made by the Entity that operates the Node)	Unique ID of Entity, Serial # of certificate to revoke	Acknowledgement (success/fail/review pending)

Function	Input Parameter(s)	Return Parameter(s)
Request replacement of existing certificate – Entity (Request to revoke and replace an Entity certificate; may only be made by the Entity that operates the node)	Unique ID of Entity, Serial # of certificate to revoke, Requested contents of the new digital certificate – See Section 3.2.1	Acknowledgement (success/fail/review pending) Copy of created certificate if success; private key will be provided to Entity out-of-band in a manner TBD.
*Create new certificate – Node	Contents of the digital certificate – See Section 3.2.1	Acknowledgement (success/fail/review pending) New certificate will be added to the Node record; Private key will be provided out-of-band in a manner TBD.
*Replace existing certificate – Node	Unique ID of Node, Serial # of certificate to revoke, Contents of the new digital certificate – See Section 3.2.1	Acknowledgement (success/fail/review pending) New certificate will be added to the Node record; Private key will be provided out-of-band in a manner TBD.
*Revoke existing certificate - Node	Unique ID of Node, Serial # of certificate to revoke	Acknowledgement (success/fail/review pending)
Request revocation of existing certificate - Node (Request to revoke Node certificate; may only be made by the Entity that operates the Node)	Unique ID of node, Serial # of certificate to revoke	Acknowledgement (success/fail/review pending)
Request replacement of existing certificate – Node (Request to revoke and replace a Node certificate; may only be made by the Entity that operates the node)	Unique ID of node, Serial # of certificate to revoke, Requested contents of the new digital certificate – See Section 3.2.1	Acknowledgement (success/fail/review pending) Copy of created certificate if success; private key will be provided to Entity out-of-band in a manner TBD.

The contracted vendor shall design and implement the user-interface components such that they maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.

3.2. Technical Requirements

3.2.1. Content Model

Each Entity record within the ELPD will contain descriptive information about that Entity, which may be used to discover Entities (whether root entities, intermediate entities, or leaf entities). Each record will also contain the entity's X.509 v3 digital certificate[vi] stored as a binary security token. Table 3.6 and Table 3.7 specify the contents of these records and digital certificates, respectively.

Table 3.6 Contents of records for registered entities

Field	Format	Description/ Comments	Example
Unique Entity ID	Number may be UUID	Unique ID assigned to the Entity Record	
Active or Inactive	Text	Is the entry currently valid	Active
Short Description	Text		Scripps Memorial
Long Description	Text		Scripps Memorial Hospital Chula Vista
Demographics	Text		
Alias(es) / DBAs	Text		Scripps Mercy Scripps Mercy Hospital
Legal Address	Composite		
Type of Entity		See Table 3.1	Hospital
National Provider ID	Text	If a healthcare entity	
Entity Validation Process and Sources	Composite		
Digital Certificate	Binary	See Table 3.7	
Created By:	Text		
Last Updated	DateTime		
Last Updated by	Text	CA staff member	
Validated contact / update person	Text		
Website address	Text		
Internet Address	Numeric		
Email Address of Contact Name	Text		
Contact Name	Text		
Telephone number and extension	Number		
Fax Number	Number		
DURSA(s) that Entity conforms to	Text	Unique identifiers and text names of the DURSA(s) that the Entity has signed (may be NULL)	
Pointer(s) to the	Node	Node(s) that serve this	

Node(s) used by the Entity	Unique IDs	Entity record (may be NULL)	
Pointers to the Entity-Transaction-Exception records for the Entity (See Section 3.1.2)	Entity-Transactio n-Exception Unique ID	Exceptions to the Transactions and interoperability protocols inherited from parent/ancestor Entities (may be NULL)	
Pointer to parent Entity record for the Entity	Entity Unique IDs	Entity that is direct parent of this Entity in the hierarchy	

Table 3.7 Contents of digital certificates for registered entities

Field	Description
Certificate Serial Number	
Subject Name	Unique ID of Entity as assigned by the CA
Issuer Name	Distinguished name of certificate authority (same as “Subject” of CA’s digital certificate)
Validity Interval	Interval will be determined by policy, TBD
Public Key	Entity’s public key
Digital Signature	Signature of certificate authority
Entity’s legal name	Text
Entity’s alternative names (DBA names, acronyms, etc.) – up to five alternatives	Text
Type of Entity	Possible values include: - Hospital - Ambulatory Clinic - Integrated Delivery Network - Health Insurer - Health Information Org. - State Agency - Messaging Intermediary (the full value set is TBD)
National Provider Identifier	If a provider facility (hospital, clinic, lab, etc.)
Entity Tax ID	Text – must be a valid federal tax ID (or equivalent unique ID)
Business Address – Full Address	Text
Business Address - City	Text (for searching)
Business Address - State	Text (for searching)

Business Address - ZipCode	Text (for searching)

Table 3.8. Contents of records that activate/inactivate inherited transactions and interoperability protocols

Entity-Transaction-Exception Unique ID	Unique ID for the record
Unique Node ID	Unique ID of the Node from which the transaction and/or interoperability protocol is inherited
Transaction ID	Unique ID of the HIE Transaction from the Node's transaction record (see Table 3.9)
Protocol Unique ID	Unique ID of the Protocol from the Transaction's protocol/address record (see Table 3.10) [may be NULL if the exception is for the entire transaction, i.e. all protocols]
Status	Active or Inactive

Each Node record within the ELPD will contain relevant information about that Node, including links to the set of transactions that the Node supports and the Node's digital certificate. Each transaction, in turn, will include the specific logical address (URL) at which the transaction is supported by the Node, as well as pointers to the relevant entries in the Services Registry that describe the interoperability protocol by which the transaction is supported. Note that a node may support a specific transaction via more than one interoperability protocol. For example, a Node may support the delivery of lab results by both the Direct Project's SMTP-based protocol and the NwHIN Exchange's HTTP/SOAP-based protocol. Figure 3.8 depicts the logical relationships among these components of a Node record.

Figure 3.8 Relationships among objects that specify the interoperability capabilities of a Node

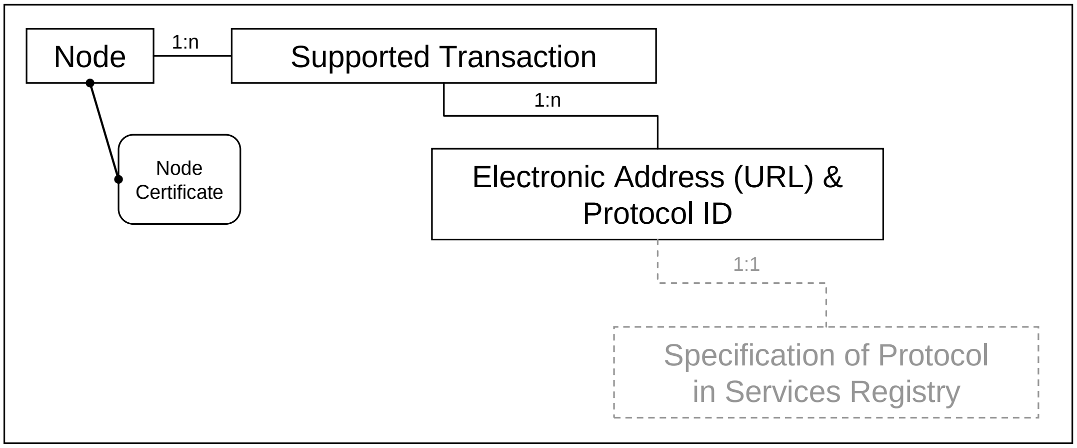


Table 3.9 to Table 3.12 specify the contents of these records and of their digital certificates, respectively.

Table 3.9. Contents of records that list the transactions supported by a registered Node

Node-Transaction Unique ID	Unique ID for the record
Transaction ID	Standard Identifier for the HIE transaction; must conform to standard naming scheme within the Cal eConnect Infrastructure (TBD); for example, "Send_Referral_Summary_Unsolicited", "Request_Discharge_Summary", etc.
Pointer(s) to Protocol/Address record(s) for the transaction	Foreign key to Protocol/Address Unique ID in Table 3.10
Conformance Attestation	Boolean (self-attestation by the Entity that operates this Node that the interoperability protocol specified in this record has been implemented in conformance with Cal eConnect specifications and is available for the indicated transaction at the indicated address)
Last Updated	Datetime
Last Updated By	Text

Table 3.10. Contents of records that specify the protocols and addresses for specific transactions

Protocol/Address Unique ID	Unique ID for the record
Unique ID of the Protocol record in the Services Registry	Pointer to the record in the Services Registry that describes the protocol that is supported at the corresponding transaction address by this node
Transaction Address	A URL specifying the logical internet address to which the transaction should be sent if the corresponding protocol is desired
Last Updated	Datetime
Last Updated By	Text

Table 3.11 Contents of records for registered Nodes

Field	Format	Description	Example
Unique Node ID	Number may be UUID	Unique ID assigned to this Node	
Active or Inactive	Text	Is the entry currently valid	Active
Created By:	Text		
Last Updated	DateTime		
Last updated by	Text		
Validated contact / update person	Text		
Secure email	Text		
Contact Name	Text		
Telephone number and extension	Number		
EMR Vendor			
EMR Type			
EMR Version			
Pointers to records of the Transactions supported by the Node	Pointer(s)	Transactions supported by this Node	

Table 3.12. Contents of digital certificates for registered nodes

Certificate Serial Number	
Subject Name	Unique ID of the Node, as assigned by the CA
Issuer Name	Distinguished name of certificate authority (same as “Subject” of CA’s digital certificate)
Validity Interval	Interval will be determined by policy, TBD
Public Key	Node’s public key
Digital Signature	Signature of certificate authority
Responsible Entity	Unique ID of the Entity responsible for operating the node

Revocation Lists: Revoked entity and node certificates will be included in X.509 Version 2 certificate revocation lists (CRLs), which will be published periodically via the ELPD (the publication schedule is TBD, pending policy decisions). Published CRLs will be signed by the certificate authority.

3.2.2. API Specifications

The technical specifications of the ELPD API will conform to the Messaging Framework and Authorization Framework specified in this document. The API for read operations will conform to the “Pull” message pattern, and the API for write operations will conform to the “Push” message pattern, as described in Section 1.1. The use of authorization artifacts for read and write transactions will conform to the specifications in Table 2.1.

.

3.2.3. Requirements for Distribution and Federation of the ELPD

The implementation of the ELPD must support federation of ELPD contents across multiple instances of the directory, with each instance storing a portion of the overall ELPD contents. The partitioning of the ELPD may be by geographical region, by Entity ID, or by other strategies which are to be determined in the course of finalizing the technical design. The goal of distributing and federating the ELPD is to enable a broad deployment of this technology (including multi-regional or even national) without the necessity for centralized administration or the creation of performance bottlenecks. In this regard, federation should approximate the architecture and functioning of the internet Domain Name System (DNS)

The federation of ELPD instances must support global search and retrieval across the aggregation of the ELPD content. Ideally, network traffic shall be managed by allowing selective escalation of queries by geographical descriptors or other suitable methods. To optimize performance, remotely discovered ELPD contents shall be cached within local ELPD instances, but only for a limited duration. If practical, the caching mechanism will include a “subscription” to the cached data at the source ELPD, such that any changes to the data at the source will be propagated to the cached versions.

3.3. Performance Requirements

The performance requirements are based on the following assumptions regarding the volume of data in the ELPD at steady state:

Entities: 30,000 – 60,000
Nodes: 50,000

The performance requirements are based on the following assumptions regarding the peak load of read and write operations:

Search for Entity Certificate by Name: 50/minute
Retrieve Entity or Node Certificate by ID: 500/minute
Retrieve Entity or Node Revocation List: 10/minute

Insert and Index Certificate (Entity or Node): 10/minute
Revoke Certificate (Entity or Node): 1/minute

Performance Requirements:

Response time per read operation: < 1 second
Response time per write operation: < 5 seconds

Availability for read and write operations: 99.999% 24x7x365

3.4. Critical Functions of Solution

The responding Bidder may propose variations to the specifications described above as long as the Bidder's specifications are functionality equivalent. The critical functions that must be met by the vendor's proposed solution are listed in Table 3.13.

Table 3.13. Critical functions of the solution for the Entity Level Provider Directory

No.	CRITICAL FUNCTIONS
ELPD-A	Entities to be represented in the ELPD:
	• HIEs, HIOs, HISPs
	• Hospitals / IDNs
	• Clinics
	• Physician offices / Groups
	• State and Federal health agencies
	• Clinical laboratories
	• Pharmacies / Pharmacy networks
	• Imaging centers
	• Health plans (including Medi-Cal, Medicare)
	• Health centers and FQHCs
	• Transaction intermediaries
	• Nursing homes
	• Home health agencies
	• Professional organizations
	• Rehabilitation facilities
	• Mental health facilities
	• Long term care facilities
	• Hospice
	• HME/DME providers
	• Other Business Associates
	• Personal health records/repositories
ELPD-1	Provide discovery of Entities and Nodes in support of the following Messaging and Authorization models: NwHIN Direct, NwHIN Exchange, Cal eConnect (i.e., as described herein)
ELPD-2	Support the certification and registration of all of the Entity types that may be engaged in health information exchange in California
ELPD-3	Represent Entities at various organizational levels, from high-level corporate entities to individual health care facilities
ELPD-4	Allow each Entity to be associated with one or more Nodes that provide health information exchange services for the Entity
ELPD-5	Represent the health information exchange capabilities of each Node (including the transactions it supports and the technical specifications of the transport, security, and message-formatting methods for each transaction type)

No.	CRITICAL FUNCTIONS
ELPD-6	Include for each node the electronic addressing information needed to send information to the Node in the context of a specific type of transaction
ELPD-7	Be highly secure and impervious to internet-based break-ins, identity spoofing, or denial of service attacks
ELPD-8	Provide both a programmatic API based on the Messaging and Authorization Frameworks described in this document, as well as a highly secure browser-based interface for direct user interaction.
ELPD-9	Require 2-factor authentication for access to the ELPD via the browser-based interface
ELPD-10	Support searching for Entities by a variety of attributes, including name, address, Entity type, NPI, tax ID, etc.)
ELPD- 11	Provide trusted, up-to-date information regarding each registered Entity’s and Node’s standing in the Cal eConnect Infrastructure, i.e. whether it is certified to conduct transactions
ELPD-12	Provide trusted, up-to-date information regarding each registered Entity’s and Node’s digital credentials, i.e. whether its digital certificate is valid or has been revoked
ELPD-13	Associate each registered Entity and Node with an X.509 class-3 digital certificate that has been signed by an authorized certificate authority
ELPD-14	Support distribution and federation of service instances to ensure acceptable performance and to allow local management within designated jurisdictions (e.g., states)
ELPD-15	Meet performance requirements
ELPD-16	All user-interface components shall be designed to maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.
ELPD-17	All application programming interfaces shall be designed to minimize the level of effort required on the part of California stakeholders and their H.I.T. vendors to integrate their solutions with the Cal eConnect infrastructure, consistent with the functional and technical requirements of these APIs

Table 3.14. Critical functions for Supporting Complex Relationships between ILPD, ELPD, and SR

No.	CRITICAL FUNCTIONS
RE-1	Each entry in the ILPD for a licensed provider may have a declared relationship with one or more entries in the ELPD. These relationships must support demographic and authorization artifacts unique to the specific relationship
RE-2	Entries in the ELPD may be hierarchical and provide for the inheritance of Node relationships created with entries higher in the hierarchy
RE-3	Each Entity may declare its own Nodes or designate the Nodes of another Entity (e.g. an HIE or HISP) as used by the Entity for a defined set of SR transactions
RE-4	If an Entity utilizes another Entities Nodes (3rd party Node), the system must allow the Entity to specify which declared services for the 3rd party Node are valid for the relationship
RE-5	Only one Node for an Entity may support a complete SR standard transaction (messaging framework, protocol, implementation guide, payload and clinical vocabulary definition)
RE-6	A Node may inherit the X.509 class-3 digital certificate from the related Entity or have its own declared certificate
RE-7	Each Node may declare that it supports one or more SR standard transactions (separately for sending and receiving) and where necessary have specific information associated with the relationship (e.g. certificate for Direct messaging protocol)
RE-8	A relationship between a Node and a SR standard transaction must provide for the ability to declare the use of an Exchange Service to translate the payload prior to sending / consuming or as a proxy agent for the communication with or from another Node

4. Services Registry

The Services Registry (SR) shall be a repository of the standard interoperability protocols supported by Entities participating in the Cal eConnect Infrastructure. Cal eConnect will specify a set of such protocols for the most important and most common transactions to be conducted via the infrastructure. Each Node registered in the ELPD will indicate which standard protocols in the Services Registry it supports (see Figure 3.8 in Section 3.2.1). Via this mechanism, participants in the Cal eConnect Infrastructure shall be able to determine the interoperability protocols that their systems must employ when exchanging health information with Providers using specific Nodes in the ELPD (the correspondence between Providers and Nodes is established via (1) mappings in the ILPD between Providers and Entities and (2) mappings in the ELPD between Entities and Nodes, as described in Section 3.1.1 and Section 6.2.1, respectively).

The information represented in the SR for each interoperability protocol will cover all levels of the OSI stack, including transport method, security model, messaging structure, and terminology system. For example, one protocol may specify an NwHIN-Direct exchange of a HITSP C32 version 2.5 CCD over REST/XDR using a TLS-encrypted session, whereas another may specify the ELINCS implementation guide (HL7 2.5.1 ORU and LOINC), for the exchange of discrete laboratory results via SOAP messaging over a TLS-encrypted session. Note that the protocols registered in the SR for use by participants in the Cal eConnect Infrastructure may include transport methods and security models other than the Messaging Framework and Authorization Framework specified in this document (for example, the NwHIN Direct transport protocol).

In the event that two Nodes have no interoperability protocols in common for a specific transaction, one or both Nodes may select an Exchange Service to translate their outbound and/or inbound transactions to one of the specified interoperability protocols (see Section 5). The Exchange Services will allow Nodes that use interoperability protocols other than those in the Services Registry to still communicate via the Cal eConnect Infrastructure in certain cases.

4.1. Functional Requirements

The SR shall be a data structure that is maintained entirely by Cal eConnect. Read access to the SR shall be available to other services operated by Cal eConnect (such as the ELPD), as well as via a web browser interface available to the public. Write access shall be available via an API and web browser, but restricted to the internal applications and personnel of Cal eConnect only.

Each record within the SR will specify a “CeC Standard Interoperability Protocol” (CSIP), which will unambiguously specify all elements of the OSI stack that comprise that protocol. CSIPs shall be defined by Cal eConnect and shall be specific to certain defined HIE transactions required to fulfill meaningful use criteria, such as

1. Deliver Laboratory Results to Ordering Provider
2. Deliver Hospital Discharge Summaries
3. Deliver Outpatient Visit Summaries
4. etc.

For example, Table 4.1 lists several example CSIPs that might be represented in the SR. Note that the contents of this table are illustrative only and the CSIPs that shall be selected for the actual SR may vary.

Table 4.1. Examples of interoperability protocols represented in the Services Registry

Transaction Type	Message Standard	Version / Transaction	Implementation Guide	Terminology Standards
Deliver Patient Summary Record [Push]	CCR			
Deliver Patient Summary Record [Push]	CCD		C32 V2.5	ICD 9 / 10 RxNorm SNOMED-CT
Transmit e-Prescription to pharmacy [Push]	NCPDP SCRIPT	8.1		Drug Terminology Mapped to RxNorm
Submit Claims for Professional Services [Push]	X.12 837	4010	CAQH CORE Rules, Phase I	
Check Insurance Eligibility [Pull]	X.12 270/271	4010	CAQH CORE Rules, Phase I	
Deliver Lab Results to Ordering Provider [Push]	HL7 ORU	2.5.1	ELINCS	LOINC
Deliver Reportable Lab Results to Public Health Agency [Push]	HL7 ORU	2.5.1	ELR2PH	LOINC, SNOMED-CT, UCUM
Submit Quality Measures [Push]	XML based		QRDA	
Submit Immunization Record [Push]	HL7	2.31. or 2.5.1		CVX
Submit Public Health Surveillance Content [Push]	HL7	2.3.1 or 2.5.1		Geocoded Interoperable

4.1.1. Read Access

The SR shall provide an API that the ELPD can use to retrieve CSIP records by their unique IDs and to search for CSIP records by various attributes, such as information type, message standard, etc.

The SR shall also provide a web browser interface available to the public, via which the standard interoperability protocols supported by the Cal eConnect Infrastructure may be discovered and inspected by Cal eConnect stakeholders. The contracted vendor shall design and implement the user-interface components such that they maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.

Because the SR contains no entity-specific, provider-specific, or patient-specific information, minimal access controls will be required for the retrieval of SR records

4.1.2. Write Access

The SR shall provide an API via which authorized services operated by Cal eConnect can create, update, and delete CSIP records. This API shall not be visible to the public internet, to prevent unauthorized updates or inadvertent corruption of the database.

The SR shall also provide a web browser interface for write access, available to authorized personnel of Cal eConnect or its contractors, via which CSIP records can be created, updated, or deleted. All modifications to the SR database shall be rigorously logged, and historical values of CSIP records shall be retained (including time stamping).

Finally, the SR shall provide a web browser interface for read access that shall be available to the general public, to enable developers of HIE Nodes and other interested parties to inspect the CSIPs.

The contracted vendor shall design and implement the user-interface components such that they maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.

4.2. Technical Requirements

4.2.1. Content Model

Table 4.2 lists the data elements that will represent CSIP records within the Services Registry, as currently envisioned. This list is subject to change and refinement as the detailed design of the SR takes place, and Cal eConnect welcomes recommendations on the final set of data elements and their manner of representation. Note that the set of Transaction Types that CSIPs support (Field #2 in Table 4.2) will be standardized and maintained by Cal eConnect as part of the contents of the Services Registry.

Table 4.2. Proposed contents of records within the Services Registry

Field	Example/ Description	Source
Unique ID	UUID	
Transaction Type	Deliver Lab Result to Ordering Provider [Push]	List of Supported Transaction Types in Services Registry
Standard Definition	CSIP	CSIP, Alt 1 … , ES 1 …
Date Established		
Established By		
Active		
Transport	Internet Protocol (IP)	List of Supported Types
Presentation	TLS/XDR	List of Supported Types

Field	Example/ Description	Source
Application	SMTP HTTPS	List of Supported Types
Protocol	HL7	List of Supported Types
Version	2.5.1	List of Supported Types
Message Type	ORU	List of Supported Types
Implementation	ELINCS	List of Supported Types
Clinical Vocabulary	LOINC	List of Supported Types

4.3. Performance Requirements

Rapid response (sub-second) for queries submitted to the SR via the API will be necessary, because such queries will be issued by the ILPD and ELPD in the course of retrieving information about registered Providers and Entities, respectively. Hence, any delay in queries submitted to the SR will degrade response times of the ILPD and ELPD. However, there shall be relatively few records in the SR (< 100), and the number of records will be under the control of Cal eConnect. Given this constraint, high performance for search and retrieval operations should not be difficult to achieve.

Write operations against the SR will be infrequent and not particularly time sensitive. A response time < 3 second for such operations shall be adequate.

4.4. Critical Functions of Solution

The responding Bidder may propose variations to the specifications described above as long as the Bidder's specifications are functionality equivalent. The critical functions that must be met by the vendor's proposed solution are listed in Table 4.3

Table 4.3. Critical functions of the solution for the Services Registry

No.	CRITICAL FUNCTIONS
SR-1	Each interoperability protocol represented in the Services Registry must include a machine-readable description of the protocol's specifications at each level of the OSI stack, including transport method, security mechanism, message format, and vocabulary constraints. This representation must be sufficiently specific to enable a software process to determine whether it can formulate and transmit a message consistent with the specified interoperability protocol
SR-2	Each interoperability protocol must be associated with a specific transaction type, and the full set of transaction types supported by the Services Registry must be defined within it
SR-3	Provide read and write access via an WS API that is available to the ELPD only
SR-4	Provide read-only access via web browser, with no access restrictions

No.	CRITICAL FUNCTIONS
SR-5	Be sufficiently secure to prevent unauthorized modification or corruption of its contents via internet-based attacks
SR-6	Meet the performance requirements as specified by Cal eConnect
SR-7	All user-interface components shall be designed to maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.
SR-8	All application programming interfaces shall be designed to minimize the level of effort required on the part of California stakeholders and their H.I.T. vendors to integrate their solutions with the Cal eConnect infrastructure, consistent with the functional and technical requirements of these APIs

5. Exchange Services

The Exchange Services (ESs) are a set of “cloud”-based services or downloadable “applets” that bridge between disparate interoperability protocols used by participants in the Cal eConnect Infrastructure. The services are intended to translate interoperability protocols (including transport specifications and message formats) and to serve as proxies and/or routing agents in health information transactions.

It is anticipated that, during the early adoption of the Cal eConnect Infrastructure, not all participants will support all of the Cal eConnect Standard Interoperability Protocols (see Section 4). For example certain participants may only support the CCD C32 document format for sending patient summaries and discharge summaries, whereas other participants may only support the CCR document format for receiving such summaries. Also, certain participants may only support HL7 v2.5.1 for sending electronic lab reports, whereas others may support only HL7 v2.3 for receiving them. The ESs shall dynamically translate among certain of these disparate protocols and formats to enable information exchange among participants that would otherwise be unable to communicate.

5.1. Functional Requirements

The vendor selected through this procurement shall develop two specific Exchange Services: A CCD/CCR Translation Service and a Lab Interoperability Hub (as described below). In the future, Cal eConnect may request the development of additional ESs, so the vendor’s proposed architecture should support the general concept of translation and routing services.

5.1.1. Specific Exchange Services to be Developed Under this Procurement

The vendor shall develop and operate two exchange services that fulfill the functional requirements described below.

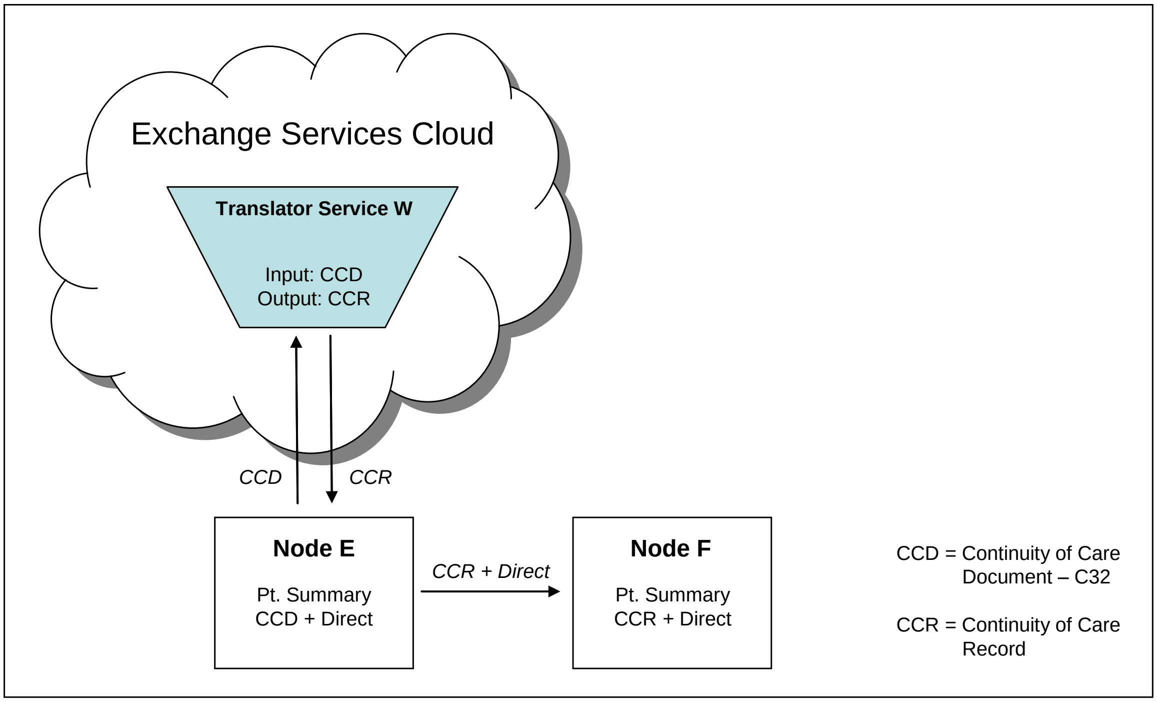
5.1.1.1. CCD-CCR Translation Service

The ES shall be able to accept a health information document (“payload”) encoded in the HITSP CCD C32 format and return an equivalent document encoded in ASTM CCR format. An Entity may use this service to translate a CCD C32 payload it has generated to the ASTM CCR format so that it may be sent to participants that can only process CCR documents. After calling the

ES to perform the translation, the Entity would then send the translated payload directly to the intended recipient using a transport and authentication protocol common to both. This type of translation will be particularly useful for sharing patient summaries and discharge summaries (which may be encoded in either CCD C32 or CCR, per the CMS EHR certification criteria). 5.1 illustrates the role of this Exchange Service.

If possible, the vendor will also implement the reciprocal capability, i.e. translation of payloads encoded in the ASTM CCR format into equivalent documents encoded in the CCD C32 format. This is a more difficult translation, because the CCD C32 format includes more detailed structure and standardized terminology than the CCR format and, in certain cases, there may be insufficient information in a specific CCR document to enable the automated generation of an equivalent CCD C32 document. However, bidding vendors should provide feedback regarding their experience with this translation and whether their bid includes a one-way or two-way Exchange Service between the CCD C32 and CCR formats.

Figure 5.1. Example of format translation services for patient summary reporting



Note that the Exchange Services shown in Figure 5.1 enable the following information flow:

Node E wishes to send a patient summary to Node F

a. Node E is an EHR system that can export only CCD C32 documents for patient summaries

b. Node F is an EHR system that can import only CCR documents for patient summaries

c. Exchange Service W is available to convert CCD C32 documents to CCR documents

d. Node F connects to Translator Service W, establishes a secure connection, and sends a CCD document to the Translator Service for conversion.

e. Translator Service W translates the CCD C32 document to a CCR document, and returns it to Node E (performing any necessary decryption/encryption required)

f. Node E uses a messaging and authorization framework also supported by Node F to envelope and transmit the CCR document to Node F, which can directly process the document.

g. Node F returns an acknowledgement directly to Node E via the messaging and authorization framework.

5.1.1.2. Lab Interoperability Hub

The ES shall provide a web service through which laboratories and EHRs can exchange test orders and test results electronically. This “hub” shall provide real-time routing, delivery, and (as needed) translation of lab-order and lab-result messages. Labs and EHRs that use the Lab Interoperability Hub shall be able to build a single interface to the hub to exchange lab orders and results with any data trading partners that also use the hub. The key functionalities of the ES will include:

1. Routing: The ES will leverage the Cal eConnect Provider Directories and/or maintain its own internal directories of labs, providers, and EHRs to determine the correct electronic end points for lab orders and results that are addressed to specific entities. For example, the ES will be able to receive a lab test result from a laboratory that is addressed to a specific provider with a specific NPI, determine the correct electronic address at which the provider can receive test results (e.g., an FTP site), and transmit the test result to that address.

2. Format Translation: The ES will be able to translate among a number of messaging standards (e.g., HL7 v2.3, HL7 v2.5.1) and implementation guides (e.g., ELINCS, ELR2PH) so that labs and EHRs using disparate standards and guides are able to exchange data reliably. For example, the ES could translate a result encoded per the ELINCS implementation guide and intended for delivery to an EHR to a semantically equivalent result encoded per the ELR2PH implementation guide and suitable for delivery to a public health agency (note: This specific translation may require that additional demographic or standardized coding information be provided as a second input).

3. Translation of Messaging and Authorization Framework: The ES will be able to translate among a small number of messaging and authorization frameworks so that labs and EHRs that support different frameworks are able to exchange data payloads. For example, the ES could translate a message transmitted using the Cal eConnect Messaging and Authorization Frameworks into an equivalent message that is compliant with the Direct Project messaging and authorization models. The translated messages could then be received by any Direct Project HISP for delivery to providers that use that type of resource. Initially, this ES shall support the following translation of messaging and authorization frameworks (1) translation from the Cal eConnect Messaging and Authorization Frameworks to the Direct Project messaging and authorization model and (2) translation from the Cal eConnect Messaging and Authorization Frameworks to the NwHIN Exchange messaging and authorization frameworks.

5.1.2. General Model for Exchange Services to be Supported by Vendor's Architecture

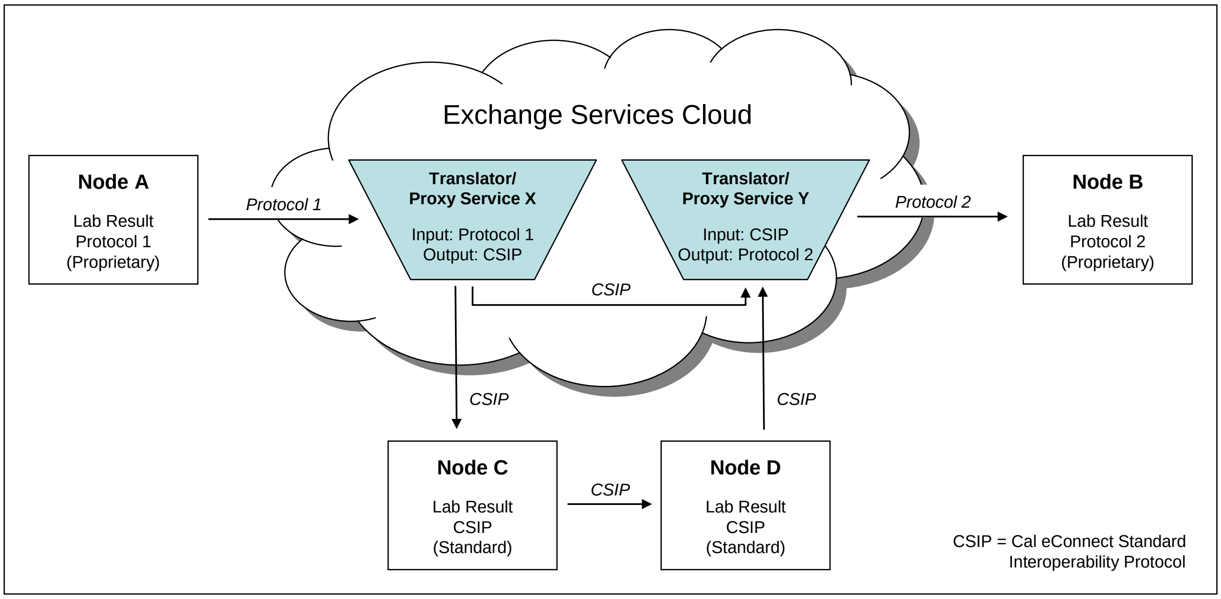
In addition to developing the specific ESs described above, the responding vendor shall also develop a technical architecture that can support the development of additional ESs in the future. This architecture should support ESs with the following general capabilities:

- Translation of messaging formats. ESs shall be able to accept a health information message ("payload") encoded in one format and return an equivalent message encoded in a different format. An Entity may use this service to translate a payload it has generated to a format that an intended recipient can process. The Entity would then send the payload directly to that recipient using a common transport and authentication protocol. There shall be a limited number of well-defined message-format translations that the ESs shall support, such as "HL7 v2.3.1 to HL7 v2.5.1" or "CCD to CCR". See Figure 5.1 for an example of how an Entity might use such an ES.

- Proxy services to translate transport and/or authorization protocols. ESs shall be able to accept a complete health information transaction sent using one transport and/or authorization protocol, translate it into a different protocol, and forward the resulting transaction to the intended recipient on behalf of the original sender. This proxy service will also translate any acknowledgements or patient data returned from the receiving Entity to the interoperability protocols of the original sender. There shall be a limited number of well-defined protocol translations that the ESs shall support, such as "Cal eConnect Messaging Framework to NwHIN Direct Protocol" or "NwHIN Direct Protocol to NwHIN Exchange Protocol." See Figure 5.2 for examples of how Entities might use such ESs.

- The ESs may translate message formats and/or protocols in varying combinations, as needed. For example, the ESs may translate a sender's proprietary protocol to a Cal eConnect Standard Interoperability Protocol and subsequently transmit the information via the standard protocol to the intended recipient. Alternatively, the ESs may first translate a sender's proprietary protocol to a Cal eConnect Standard Interoperability Protocol and then translate this standard protocol to yet another proprietary protocol recognized by the intended recipient and send the information to that recipient. Figure 5.2 shows several combinations of transformations that may be supported by Exchange Services.

Figure 5.2. Example of protocol translation and proxy services for lab result reporting



Note that the Exchange Services shown in Figure 5.2 enable the following information flows:

1. Node C wishes to send lab results to Node D
    a. Both Nodes support the CSIP for Lab Results over a SOAP service.
    b. Node C creates a secure connection directly to Node D and sends the Lab Results
2. Node A wishes to send lab results to Node C
    a. Node A is a Lab system that supports only Protocol 1
    b. Node C is an EHR system that supports the CSIP for Lab Results
    c. Translator/Proxy Service X is available (specific to Node A) to convert Protocol 1 to the CSIP for Lab Results
    d. Node A connects to Translator/Proxy Service X via a SOAP connection, establishes a secure non-repudiation link, sends the Unique Node Address of the intended recipient (Node C) and the laboratory results using Protocol 1
    e. Translator/Proxy Service X converts the laboratory results and messaging/authorization protocol to the CSIP, and creates a proxy session with Node C on behalf of Node A. The Translator/Proxy Service then sends the information with the digital certificate and signatures of the sending Entity and Provider (if necessary).
    f. Any acknowledgement is returned to the sender via Translator/Proxy Service X

3. Node A wishes to send lab results to Node B

   (Steps a to c are the same as Node A to Node C)

   d. Node A connects to Translator/Proxy Service X via a SOAP connection, establishes a secure non-repudiation link, sends the Unique Node Address of the intended recipient (Node B) and the laboratory results using Protocol 1

   e. Translator/Proxy Service X converts the laboratory results and messaging/authorization protocol to the CSIP. Since the recipient Node (Node B) only accepts lab results sent per Protocol 2, Translator/Proxy Service X sends the information (including the sender and recipient information) to Translator/Proxy Service Y, which is the indicated Exchange Service for translating laboratory results for Node B.

   f. Translator/Proxy Service Y converts the CSIP to the protocol acceptable to Node B (Protocol 2).

   g. Translator/Proxy Service Y creates a proxy session with Node B on behalf of Node A and then sends the information with the digital certificate and signatures of the sending Entity and Provider (if necessary).

   h. Any acknowledgement is returned to the sender via Translator/Proxy Service Y and Translator/Proxy Service X.

4. Node D wishes to send lab results to Node B

   a. Node D determines the required Exchange Service from Node B’s record for lab results in the Services Registry (i.e., Translator/Proxy Service Y). Node D connects to Translator/Proxy Service Y.

   b. The transactions proceed the same steps f) – h) in the previous example

In the future, the set of available Exchange Services shall be listed in a registry accessible to participants in the Cal eConnect Infrastructure. As with the other core services of the Cal eConnect Infrastructure, the Exchange Services Registry shall be accessed using the Messaging Framework and Authorization Framework described in Sections 1 and 2 of this document. Table 5.1 shows the proposed contents of entries in the Exchange Services Registry (provided as an example only).

Table 5.1. Proposed contents of Exchange Services Registry

Field	Definition / Type	Content	Source
ES Unique ID	UUID		Assigned on insert
Status	Text	Active	List
Short Description	Text	CCD C32 to CCR	
Long Description	Text	Conversion of HITSP CCD C32 to ASTM CCR	
Information Content	Laboratory Results	Patient data summary	List of Information Content
Source Standard	CSIP standard format	CDA + CCD + HITSP C32	SR
Sink Standard	CSIP standard format	ASTM CCR	SR
Input CSIP	Byte	Y or N	List
Output CSIP	Byte	Y or N	List
Date Established	DateTime		
Established By	Authorized CeC user		
Translation Tables	Links to Translations		

5.2. Critical Functions of Solution

The responding Bidder may propose variations to the specifications described above as long as the Bidder's specifications are functionality equivalent. The critical functions that must be met by the vendor's proposed solution are listed in Table 5.2.

Table 5.2. Critical functions of the solution for the Exchange Services

No.	CRITICAL FUNCTIONS
ES-1	Translate message formats and transport/authentication mechanisms to semantically equivalent versions
ES-2	When acting as a proxy, must fully conform to the interoperability protocols of the sending and receiving Entities, so that these entities may generate and process the information (respectively) as if it had been sent directly from the source to the target
ES-3	When acting as a proxy, must pass through all required information and artifacts needed by the recipient to validate the sender and make authorization decisions (although the proxy may validate the sender on behalf of the recipient if it formally attests to the validation)
ES-4	When acting as a proxy, must appropriately translate and deliver any acknowledgements or other data returned from the recipient to the sender
ES-5	All application programming interfaces shall be designed to minimize the level of effort required on the part of California stakeholders and their H.I.T. vendors to integrate their solutions with the Cal eConnect infrastructure, consistent with the functional and technical requirements of these APIs

6. Individual Level Provider Directory

The Individual Level Provider Directory (ILPD) is a secure directory of information about providers that participate in the Cal eConnect Infrastructure and Trust Framework. The ILPD contains information that describes providers and provides search functions that enable the discovery and lookup of provider information. The ILPD also specifies the Entity or Entities with which providers are associated, enabling client applications to retrieve relevant information from the ELPD needed to conduct HIE transactions with specific providers (as described in Section 3). The ILPD provides both a web services API and a web browser interface for the reading and writing of this information. The means by which providers in the ILPD are associated with entities in the ELPD is described in Section 6.2.1.2.

Like the ELPD, the ILPD will be provided by Cal eConnect as a central shared resource to support HIE.

The sections below describe the functional, technical, and performance requirements of the ILPD.

6.1. Functional Requirements

The ILPD supports both read and write access via a web services API. The term "Provider" is applied generally in the context of the ILPD, and it may refer to an individual person (such as a physician, other clinician, or administrative professional), an organizational unit (such as an emergency department), or an information resource (such as an immunization registry). *Note that the term does not necessarily refer to a physician or other health care provider.*

To provide comprehensive access to the Cal eConnect services, the following Provider types shall be included in the ILPD:

Table 6.1. Types of providers to be represented in the ILPD

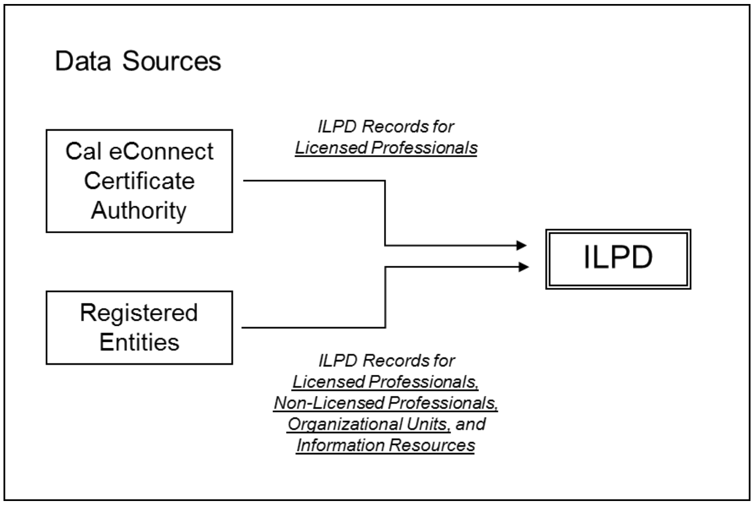
Priority	Type of Provider	Estimated Number in CA
1	Medical Doctors	126,000
	Osteopathic Physicians	Incl
	Registered Nurses	TBD
	Clinical Units (that receive PHI)	TBD
	Information Resources	TBD
2	Optometrists	TBD
	Dentists	TBD
	Dental Assistants	TBD
	Podiatrists	TBD
	Chiropractors	TBD
3	LPNs	TBD
	Administrators (with rights)	TBD
	Other Individuals and Entities	TBD

For providers who are licensed professionals (MDs, DOs, Pharmacists, etc.), the ILPD will maintain a unique identity for each individual, regardless of the various Entities with which the individual may be associated. Cal eConnect may certify and credential these individuals itself in the course of creating their ILPD records. In this sense, the ILPD will serve as a certificate authority. However, entities may also register licensed professionals in the ILPD themselves and “self-attest” to the identity of these individuals (i.e., without Cal eConnect certification and credentialing). In these cases, the entities alone will serve as the certificate authorities for these licensed professionals. In either case, the ILPD will include identity matching and de-duplication capabilities to maintain a single ILPD record for every licensed professional. Hence, the ILPD will maintain a “Master Provider Index” for licensed professionals within the statewide healthcare system, regardless of the source(s) of the professionals’ registration data.

For providers who are unlicensed individuals, organizational units, or information resources, the ILPD will store information provided by the Entity or Entities with which the providers are associated. This information will not be certified by Cal eConnect, beyond the requirements that Cal eConnect places on all Entities to furnish accurate provider information in the ILPD. As for licensed professionals, Entities will be able to submit Provider records to the ILPD for these provider types without centralized certification or credentialing. Although this practice may result in multiple records in the ILPD for the same provider, this multiplicity will be mitigated by the identity-matching and de-duplication functions available within the ILPD.

Figure 6.1 illustrates the sources of ILPD records based on the type of provider. Note that, although the Cal eConnect Certificate Authority must insert the official records for licensed professionals in the ILPD, the information used to populate these records may be provided directly by the professionals of by the professionals' Entities (which can serve as "proxies" for submitting this information, to facilitate the process for the professionals and to obviate the need for Cal eConnect to certify and credential them).

Figure 6.1 Sources of ILPD records for various provider types


Data Sources
Cal eConnect Certificate Authority
ILPD Records for Licensed Professionals
ILPD
Registered Entities
ILPD Records for Licensed Professionals, Non-Licensed Professionals, Organizational Units, and Information Resources

6.1.1. Read Access via API

Read access to the ILPD is available only to providers who belong to certified entities and use certified nodes. Read access to the ILPD is more tightly controlled than read access to the ELPD to prevent the "mining" of provider data, identity theft, etc.. The retrieval of information from the ILPD is intended to meet the following needs of participants in the Cal eConnect infrastructure:

1. Determination of whether a Provider is registered in the ILPD as a certified Provider approved to participate in the Cal eConnect infrastructure.
2. Determination of the electronic identity and attributes of a provider with which a participant would like to exchange information. This query will enable HIE participants to discover a provider's ILPD record (and access the information therein) when the provider's unique ID is not known.
3. Determination of the Entities with which a specific Provider is associated, and the identifying attributes and security credentials for that Provider in the context of the Entity (e.g., a local identifier and/or digital certificate assigned by the Entity).
4. For each Entity with which a Provider is associated, access to the Entity's record in the ELPD, to retrieve the attributes of the Entity (including its Node(s)) and to determine

whether the Entity is certified by Cal eConnect and has an active Digital Certificate for the Cal eConnect Infrastructure.

To meet these needs, the ILPD will provide the following web-service functions:

Table 6.2 API functions for read access to ILDP

Function	Input Parameter(s)	Return Parameter(s)
Search for Provider by Provider attributes	Search Attribute(s): - Provider Type - Provider Full Name - Unique ID of an Entity with which Provider is associated - NPI (if applicable) - Name of an Entity with which Provider is associated - Location (city, zip code, or state) of an Entity with which Provider is associated [Provider Full Name or NPI are required search terms]	Matching Provider record(s) (see Section 6.2.1.1) + all ILPD/ELPD mapping records for that provider
Search for Provider record by Unique ID	Unique ID of Provider as assigned by ILPD	Matching Provider record (see Section 6.2.1.1)
Retrieve Entities associated with Provider (i.e., search within ILPD only)	Unique ID of Provider as assigned by ILPD	ILPD/ELPD mapping record for each Entity associated with the Provider (see Section 6.2.1.26.2.1.2) + the corresponding Entity record from the ELPD
Retrieve Node(s) corresponding to an Entity	Unique ID of Entity as assigned by ELPD	Node record(s)
Retrieve revocation list for Provider certificates issued by Cal eConnect or Entities	Date of last revocation list retrieval (may be NULL)	All revocation list(s) since date of last retrieval (or, if no date provided, all revocation lists)

As specified in Table 2.1, a number of authorization artifacts are required for requesting information from the ILPD.

The data structure and contents of Provider records are specified in Section 6.2.1.1.

6.1.2. Read Access via Web Browser

In addition to a web-services API, the ILPD will also support read access from web browsers. This capability will allow Providers to access information in the ILPD directly via the internet for purposes of discovering their counterparties in H.I.E. transactions and determining which transactions and interoperability protocols these counterparties support. Table 6.3 lists the read operations that will be available via web browser.

Table 6.3. Web-browser operations for read access to ILPD

Function	Input Parameter(s)	Return Parameter(s)
Search for Provider by Provider attributes	Search Attribute(s): - Provider Type - Provider Full Name - Unique ID of an Entity with which Provider is associated - NPI (if applicable) - Name of an Entity with which Provider is associated - Location (city, zip code, or state) of an Entity with which Provider is associated [Provider Full Name or NPI are required search terms]	"Header information" from each matching Provider record(s) and associated Entities, including Provider name, specialty, and work location(s)
Search for Provider record by Unique ID	Unique ID of provider as assigned by ILPD	Web-displayable data from matching Provider record (see Section 6.2.1.1)
Retrieve Entities associated with Provider (i.e., search within ILPD only)	Unique ID of Provider as assigned by ILPD	Web-displayable data from ILPD/ELPD mapping record for each Entity associated with the Provider (see Section 6.2.1.2) + the corresponding Entity record from the ELPD (see Section 3.2.1)
Retrieve Node(s) corresponding to an Entity	Unique ID of Entity as assigned by ELPD	Web-displayable data from Node record(s)

Read access to the ILPD via web browser will only be available to Providers registered in the ILPD, to avoid disclosure of directory information to the general public or parties with malicious intent (e.g., identity theft). Read access to individual Provider records and ILPD/ELPD mapping records will be rigorously logged by the ILPD.

The contracted vendor shall design and implement the user-interface components such that they maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.

6.1.3. Write Access via API

Write access to the ILPD is also tightly controlled and confined to authenticated Providers accessing the ILPD from a registered Entity. Any create, update, or delete operations against the ILPD will be strictly logged for auditing purposes. All historical values of ILPD records must be maintained, with appropriate datetime stamps indicating the interval during which these values were current.

The writing of information to the ILPD is intended to meet the following needs of the HIE infrastructure:

1. Creating, editing, and deleting Provider records for those licensed providers that have been certified by Cal eConnect. These operations will be limited to staff of the Cal eConnect certificate authority. Once such a record is created for a licensed provider, the provider may be associated with one or more Entities.

2. Creating, editing, and deleting Provider records for those licensed professionals that have been certified by a registered entity other than Cal eConnect. These operations will be available to any registered Entity.

3. Requesting that an association be created between a licensed Provider already represented in the ILPD and a certified Entity already represented in the ELPD. These requests may be made by either a Provider or by an Entity, and must be authorized by both parties before the association is committed to the ILPD/ELPD Mapping Database (see Section 6.2.1.2).

4. Creating, editing, and deleting Provider records for those non-licensed professionals, organizational units, and information resources that an entity wishes to publish via the ILPD. These operations enable Entities to make widely available the electronic identity and contact information of their non-licensed providers without requiring these providers to be certified by Cal eConnect

It is important to note that ILPD Provider records for licensed professionals (primarily physicians) may be created in one of two ways:

1. By Cal eConnect in response to a direct request by the professional, in which case Cal eConnect itself will certify the identity of the professional and issue a digital certificate based on that identity. In this case, the Provider record in the ILPD will be associated with a digital certificate signed by Cal eConnect.

2. By an Entity on behalf of a licensed professional who is already associated with the Entity, in which case the Entity will certify the identity of the professional and issue a digital certificate based on that identity. In this case, the Entity will directly create an ILPD/ELPD mapping record rather than an ILPD Provider record (see the content model described in Section 6.2.1 for the distinction between these two record types). Specifically, an Entity will submit a new ILPD/ELPD mapping record containing the local identifiers, attributes, and security credentials of a licensed professional that the Entity has certified and credentialed. If a record already exists in the ILPD for the submitted professional, the ILPD matching engine will automatically detect this and associate the newly submitted ILPD/ELPD matching record with the existing Provider record of the professional. Otherwise, the ILPD will create a new Provider record for the professional based on the information in the ILPD/ELPD mapping record that the Entity has provided. In either case, the submitted ILPD/ELPD mapping record will create an association between the Entity that submitted it and the Provider that was submitted.

For unlicensed professionals, organizational units, and information resources, ILPD records are directly created by the Entities to which these Providers belong, along with the ILPD/ELPD mapping records that associate these Providers with the submitting Entities. In this case, however, the Provider record of a non-licensed professional, organizational unit, or information resource cannot be associated with any other Entity (unlike that of a licensed professional).

To meet these needs, the ILPD will provide the following web-service functions:

Table 6.4. API functions for write access to ILPD

Function	Input Parameter(s)	Return Parameter(s)
Insert new licensed Provider record (Cal eConnect)	Provider record (See Section 6.2.1.1)	Acknowledgement (success/fail)
Update existing licensed Provider record (Cal eConnect)	Unique ID of existing provider record, Updated provider record	Acknowledgement (success/fail)
Inactivate existing licensed Provider record and all child Provider/Entity associations (Cal eConnect)	Unique ID of existing provider record	Acknowledgement (success/fail)
Insert new licensed Provider record (Entity)	ILPD/ELPD mapping record (See Section 6.2.1.2)	Acknowledgement (success/fail)
Update existing licensed Provider record (Entity)	Unique ID of ILPD/ELPD mapping record, updated content of ILPD/ELPD mapping record	Acknowledgement (success/fail)
Inactivate existing licensed Provider record (Entity)	Unique ID of ILPD/ELPD mapping record	Acknowledgement (success/fail)
Request association of licensed Provider with certified Entity (made by Provider)	Unique ID of an existing Entity	Acknowledgement (success/fail)
Approve request made by Provider for association with certified Entity (granted by Entity)	Unique ID of existing Provider, new ILPD/ELPD mapping record	Acknowledgement (success/fail)
Request association of licensed Provider with certified Entity (made by Entity)	Unique ID of existing Provider, new ILPD/ELPD mapping record	Acknowledgement (success/fail)

Function	Input Parameter(s)	Return Parameter(s)
Approve request made by Entity for association with licensed Provider (granted by Provider)	Unique ID of an existing Entity	Acknowledgement (success/fail)
Insert new non-licensed Provider record (Entity)	Provider record and corresponding ILPD/ELPD mapping record (See Section 6.2.1.2)	Acknowledgement (success/fail)
Update existing non-licensed Provider record (Entity)	Unique ID of existing provider record, Updated provider record and/or updated corresponding ILPD/ELPD mapping record	Acknowledgement (success/fail)
Inactivate existing non-licensed Provider record and corresponding ILPD/ELPD mapping record	Unique ID of existing provider record	Acknowledgement (success/fail)

The data structures and contents of Provider records and ILPD/ELPD mapping records are specified in Section 6.2.1.

As specified in Table 2.1, a number of authorization artifacts are required to update information in the ILPD. In addition, all such updates and requests for updates will be rigorously logged by the ILPD.

6.1.4. Write Access via Web Browser

In addition to a web-services API, the ILPD will also support write access from web browsers. This capability will allow Providers and/or Entities to create, modify, or delete information in the ILPD that they earlier provided. For example, an Entity would be able to change the contact information for a non-licensed provider or the digital certificate for an information resource that it previously entered into the ILPD. This capability will also allow Providers or Entities to request associations with existing Entities or Providers, respectively. Note that personnel of Cal eConnect will also have a web-browser interface for creating and editing Provider records for licensed professionals. Table 6.5 lists the write operations that will be available via web browser for the ILPD.

Table 6.5. Web-browser operations for write access to ILPD

Operation	Input Parameter(s)	Return Parameter(s)
Insert new licensed Provider record (by Cal eConnect Certificate Authority)	Data elements required to populate a Provider record	Acknowledgement (success/fail)
Update existing licensed Provider record (by Cal eConnect Certificate Authority)	Unique ID of existing provider record, Updated data elements for provider record	Acknowledgement (success/fail) Fail if record was not created by Cal eConnect Certificate Authority
Inactivate existing licensed Provider record and corresponding ILPD/ELPD Mapping records record (by Cal eConnect Certificate Authority)	Unique ID of existing provider record	Acknowledgement (success/fail) Fail if record was not created by Cal eConnect Certificate Authority
Insert new licensed Provider record (by Entity)	ILPD/ELPD mapping record (See Section 6.2.1.2)	Acknowledgement (success/fail)
Update existing licensed Provider record (by Entity)	Unique ID of ILPD/ELPD mapping record, updated content of ILPD/ELPD mapping record	Acknowledgement (success/fail) Fail if record was not created by the Entity
Inactivate existing licensed Provider record (by Entity)	Unique ID of ILPD/ELPD mapping record	Acknowledgement (success/fail) Fail if record was not created by the Entity
Request association of licensed Provider with certified Entity (made by Provider)	Unique ID of an existing Entity	Acknowledgement (success/fail)
Approve request made by Provider for association with certified Entity (granted by Entity)	Unique ID of existing Provider, data elements for new ILPD/ELPD mapping record	Acknowledgement (success/fail)
Request association of licensed Provider with certified Entity (made by Entity)	Unique ID of existing Provider, data elements for new ILPD/ELPD mapping record	Acknowledgement (success/fail)

Operation	Input Parameter(s)	Return Parameter(s)
Approve request made by Entity for association with licensed Provider (granted by Provider)	Unique ID of an existing Entity	Acknowledgement (success/fail)
Insert new non-licensed Provider record (Entity)	Data elements required to populate a Provider record and corresponding ILPD/ELPD mapping record	Acknowledgement (success/fail)
Update existing non-licensed Provider record (Entity)	Unique ID of existing provider record, Updated data elements for provider record and/or updated data elements for corresponding ILPD/ELPD mapping record	Acknowledgement (success/fail)
Inactivate existing non-licensed Provider record and corresponding ILPD/ELPD Mapping record	Unique ID of existing provider record	Acknowledgement (success/fail)

Write access via web browser will in all cases require two-factor authentication of the end user, because the messaging and authentication framework will not be used in this mode of interaction with the ILPD. Users (Providers) who wish to make changes to the ILPD via web browser will need to be certified by Cal eConnect and be assigned suitable credentials for two-factor authentication (even if they are non-licensed providers). Also, any updates to the ILPD via web browser will be rigorously logged.

The contracted vendor shall design and implement the user-interface components such that they maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.

6.2. Technical Requirements

6.2.1. Content Model

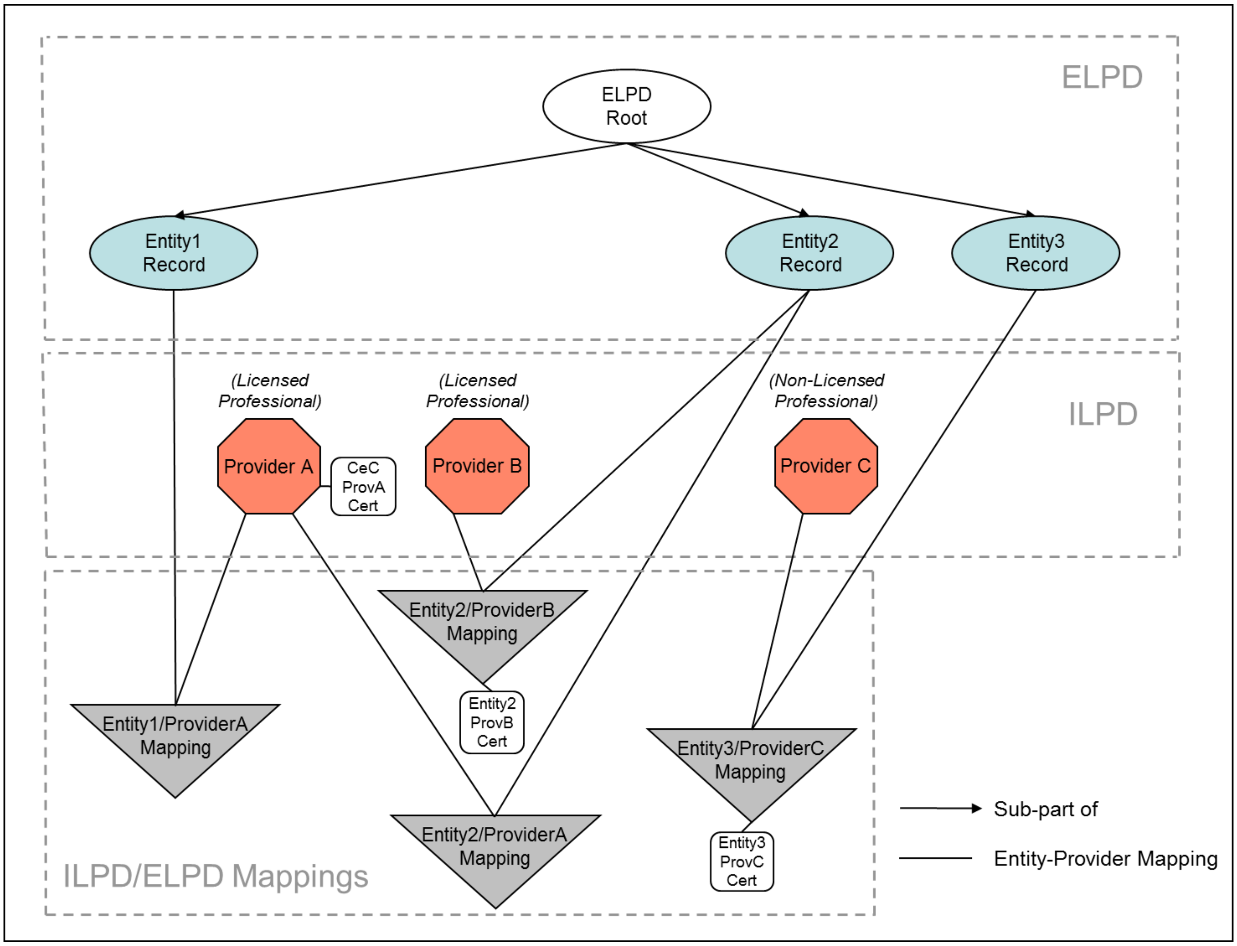
The content model comprises Provider records in the ILPD itself, as well as ILPD/ELPD mapping records. The latter represent the associations between Provider records in the ILPD and Entity records in the ELPD. Figure 6.2 illustrates the relationships among these objects given several situations.

Provider A represents a licensed professional, whose ILPD record was created by the Cal eConnect certificate authority and subsequently associated with two different entities (Entity1 and Entity2) at the request of the Provider. Provider A, therefore, has a digital certificate issued by Cal eConnect ("CeC ProvA Cert").

Provider B is a licensed professional who was certified and whose ILPD/ELPD Mapping record was created by Entity2 and directly added to the ILPD/ELPD mapping database. The addition of that ILPD/ELPD mapping record caused the ILPD matching engine to automatically create a corresponding ILPD Provider record for the licensed professional, because that professional's identity did not yet exist in the ILPD. Provider B has only a digital certificate issued by Entity2 ("Entity2 ProvB Cert"). If another Entity were to also add an ILPD/ELPD Mapping record for Provider B, the ILPD would detect that an ILPD record already existed for that Provider and simply associate the existing ILPD record with the added ILPD/ELPD mapping record, rather than create a new (duplicate) ILPD record. If Entity2 were to delete the ILPD/ELPD mapping record for Provider B, the ILPD would automatically inactivate the ILPD record for Provider B, because that provider would no longer be associated with any Entity (and therefore could not participate in HIE). However, Provider B could at that point request that Cal eConnect certify her identity and issue her a digital certificate, subsequent to which Provider could request association with any other Entity (just as Provider A can).

Provider C represents a non-licensed professional, who was certified and whose ILPD record was created by Entity3 and directly added to the ILPD by that Entity. Provider C, therefore, only has a digital certificate issued by Entity3 ("Entity3 ProvC Cert"). Provider C cannot request that Cal eConnect certify his identity and issue him a digital certificate, because he is a non-licensed professional and therefore his identity cannot exist independently of the Entity that originally created his ILPD record.

Figure 6.2. Relationship among objects in the ILPD, ELPD, and ILPD/ELPD Mapping Component



Default association with Cal eConnect Entity: Every licensed Provider with a record in the ILPD and a digital certificate issued by Cal eConnect will be granted a “default” association with the built-in Entity “Cal eConnect” at the time the Provider’s record is created in the ILPD (this association is omitted from Figure 6.2 to simplify the diagram). The Cal eConnect Entity will operate a Node intended to support basic communications, such as Providers’ requests to establish associations with other Entities (see Section 7.1.1). This default association with the Cal eConnect Entity is necessary because the messaging and authorization frameworks described in Section 1 and Section 2 require every communication to take place via a registered Entity and a registered Node, but a newly created licensed Provider record will initially have no associations with any Entity or Node. Hence, the default association with the Cal eConnect Entity and Node will enable the communications required to establish further associations (and possibly other basic operations, such as secure email, which may be provided by Cal eConnect independently of other Entities – See Section 7).

6.2.1.1. Provider Record

Each Provider record will contain the fields specified in Table 6.6., Table 6.7, and Table 6.8. Note that the specific fields within a provider record and certificate will vary by the provider type, so that the fields in Table 6.6 **Error! Reference source not found.**represent the "union" of all fields that may apply to a provider, although only certain of the fields will be populated for each specific type of provider (per the specifications in Table 6.8).

Table 6.6. Fields to be included in Provider records

Field	Format	Public	Description
Unique Provider ID	UUID	No	Assigned by System
Active or Inactive	Byte		Is this an active provider
Last Name	Text	Yes	
First Name	Text	Yes	
Middle Name or Initial	Text	Yes	
Prefix	List	Yes	
Suffix	List	Yes	
Primary Business Address	Composite	Yes	
Personal Address	Composite		
Primary Business Telephone	Telephone Number	Yes	
Home Telephone	Telephone Number		
Mobile Phone Number	Telephone Number		
Answering Service	Telephone Number	Yes	
Preferred Email	Email		
Date of Birth	Date	Yes	
Gender	Byte	Yes	
Degree/Title	Text	Yes	
Last updated by	Text		
Last update date	DateTime		
NPI number	Number	Yes	
DEA number	Number		

Field	Format	Public	Description
CDS number	Number	Yes	
CA Lic. Number	Number	Yes	
Specialties	Text or Lists	Yes	
Tax ID Number	Number		
Last Accessed	DateTime		
Number of Accesses	Number		
Proxy for Updates	Composite		
Digital Certificate	Binary	Yes	Created and signed by CeC Cert. Auth. (if one exists for this Provider)
Address of ILPD/ELPD Mapping Database(s) (URL(s))	Text (multi-valued)	Yes	Indicates address of web service(s) that store the ILPD/ELPD Mapping Records for this Provider. In initial version of ILPD, will default to the ILPD/ELPD Mapping Database operated by Cal eConnect. May later point to other Mapping Databases operated by Entities, themselves, or by third parties.

Table 6.7. Fields to be included in Provider digital certificates

Fields	Value Set/Comments
Unique Provider ID	Unique ID assigned by CA or an Entity, depending on the type of Provider
Date created	
Digital Signature	Signature of signing entity. Must validate using the public key of the entity to which the provider belongs, per the entity component of the Provider Unique ID
<Remaining attributes depend on the provider type >	See Table 6.8 for details.

Table 6.8. Provider attributes to be included in Provider record, by provider type.

Provider Type	Attribute	Value Set/Comments
LicensedProvider (Physician, pharmacist, DO, etc.)	First Name	Text
	Last Name	Text
	Middle Initial or Name	Text (optional)
	Professional Degree	Text (“MD”, “DO”, etc.)
	NPI	CMS NPI
	Specialty	Text name of specialty
	Relevant Institution	Text name of institution
	Institution Address	Text address, including street, city, etc.
	Contact Phone Number	10-digit phone number
	Contact Email Address	Text (optional)
NonLicensedProvider (non-licensed clinicians and administrative users)	(Same attributes as LicensedProfessional, except that NPI, Professional Degree, and Specialty are optional)	Assigned by Entity that created the certificate
Proxy (a provider that is conducting an HIE transaction on behalf of another provider)	First Name	Text
	Last Name	Text
	Middle Initial or Name	Text (optional)
	Provider Type	Text (any of the provider types indicated in this table, except “Proxy”)
	Relevant Institution	Text name of institution
	Institution Address	Text address, including street, city, etc.
	Contact Phone Number	10-digit phone number
	Contact Email Address	Text (optional)
	On-Behalf-Of-Provider	Full set of attributes (as specified in this table) for the provider whom the proxy is representing in the specific transaction
OrganizationalUnit (A department, unit, site, etc. of an entity that may be the	Name	Text
	Description	Text
	Parent Institution	Text

recipient or sender of health information)	OrganizationalUnit Address	Text address, including street, city, etc.
	Organizational Unit Contact Name	Text
	OrganizationalUnit Contact Provider Unique ID	Text
	Organizational Unit Contact Phone Number	10-digit phone number
	OrganizationalUnit Contact Email Address	Text (optional)
	Unique Provider ID	Assigned by Entity that created the Organizational Unit entry
InformationResource (e.g., an immunization registry, disease registry, public health surveillance system, etc.)	Name	Text
	Description	Text
	Parent Institution	Text

Note: The list of Provider Types above is not necessarily complete

6.2.1.2. ILPD/ELPD Mapping Record

Each IPLD/ELPD mapping record shall contain the fields specified in Table 6.9. These records shall be managed by and maintained within the ILPD/ELPD Mapping Database, which shall be accessible to both the ILPD and the ELPD (although the Cal eConnect Infrastructure shall provide no public interface to this database). These records shall represent the associations between Providers and Entities, which shall be used to (1) retrieve all Entity and Node information for Providers who have been discovered via the ILPD, and (2) search for Providers in the context of a specific Entity.

Table 6.9. Fields to be included in ILPD/ELPD mapping record

Field	Format	Description	Example
Unique Provider ID	UUID	Unique ID assigned to the Provider in the ILPD	
Provider Type	Text	See table 6.8 for list of provider types	
Unique Entity ID	UUID	Unique ID assigned to an Entity in the ELPD	
Active or Inactive	Text	Is the entry currently valid	Active
Validated by Provider	Boolean		

Field	Format	Description	Example
Validated Provider contact / update person	Composite	Name, contact info	
Validated by Entity	Boolean		
Validated Entity contact / update person	Composite	Name, contact info	
Contact information	Composite	Provider contact Info specific to this relationship	May be NULL
Provider Local ID	Composite	Provider ID specific to this relationship; should be used as value of TO and FROM address in communications with Provider at this Entity	May be NULL
Email Address	Text	Provider email address specific to this relationship	May be NULL
<Additional fields, depending on Provider type - see Table 6.8>	<variable>	See Table 6.8	
Provider Local Certificate	Text	Provider digital certificate specific to this relationship; Should be used in H.I.E. transactions with Provider at this Entity	May be NULL
Created By:			
Last Update			
Last updated by			

6.2.2. API Specifications

The technical specifications of the ILPD API will conform to the Messaging Framework and Authorization Framework specified in this document. The API for read operations will conform to the “Pull” message pattern, and the API for write operations will conform to the “Push” message pattern, as described in Section 1.1. The use of authorization artifacts for read and write transactions will conform to the specifications in Table 2.1.

6.2.3. Requirements for Distribution and Federation of the ILPD

The implementation of the ILPD must support federation of ILPD contents across multiple instances of the directory, with each instance storing a portion of the overall ILPD contents. The partitioning of the ILPD may be by geographical region, by Provider name, or by other strategies that are to be determined in the course of finalizing the technical design. The goal of distributing and federating the ILPD is to enable a broad deployment of this technology (including multi-regional or even national) without the necessity for centralized administration or the creation of performance bottlenecks. In this regard, federation should approximate the architecture and functioning of the internet Domain Name System (DNS).

The federation of ILPD instances must support global search and retrieval across the aggregation of the ILPD content. Ideally, network traffic shall be managed by allowing selective escalation of queries by geographical descriptors or other suitable methods. To optimize performance, remotely discovered ILPD contents shall be cached within local ILPD instances, but only for a limited duration.

6.3. Performance Requirements

The performance requirements are based on the following assumptions regarding the volume of data in the ILPD at steady:

Providers: 500,000
Entities: 30,000 – 60,000

The performance requirements are based on the following assumptions regarding the peak load of operations against the ILPD:

Search for Provider by attributes: 50/minute
Retrieve Provider record by Provider ID: 500/minute
Retrieve Entity record(s) by Provider ID: 100/minute
Retrieve Node record(s) by Entity ID: 100/minute

Insert and index licensed-Provider record: 10/minute
Insert and index ILPD/ELPD mapping record for licensed Provider: 25/minute
Insert and index non-licensed-Provider record and corresponding ILPD/ELPD mapping record:
50/minute
Insert and index : 1/minute

Performance Requirements:

Response time – Provider search operation: < 3 second
Response time – Provider record retrieval operation: < 1 second
Response time – Provider Entity retrieval operation: < 1 second

Response time – Provider Node retrieval operation: < 1 second
Response time for all write operations (API or web browser): < 3 seconds

Availability for read and write operations: 99.999% 24x7x365

6.4. Critical Functions of Solution

The responding Bidder may propose variations to the specifications described above as long as the Bidder's specifications are functionality equivalent. The critical functions that must be met by the vendor's proposed solution are listed in Table 6.10.

Table 6.10. Critical functions of the solution for the Individual Level Provider Directory

No.	CRITICAL FUNCTIONS
ILPD-A	Types of providers to be represented in the ILPD:
	• Medical Doctors
	• Osteopathic Physicians
	• Registered Nurses
	• Clinical Units (that receive PHI)
	• Information Resources
	• Optometrists
	• Dentists
	• Dental Assistants
	• Podiatrists
	• Chiropractors
	• LPNs
	• Administrators (with rights)
	• Other Individuals and Entities
ILPD-1	Accommodate "providers" who are licensed clinicians, unlicensed clinicians, administrative personnel, organizational units, and information resources
ILPD-2	Support identity-validation and digital credentialing services for licensed clinicians, such that these providers' entries in the ILPD will serve as official records of the providers' digital identity
ILPD-3	Support representation of invalidated identity information provided by trusted Entities for unlicensed clinicians and non-clinician providers
ILPD-4	Support representation of invalidated identity provided by trusted Entities for licensed professionals, and automatically determine whether the information represents a new identity in the ILPD (in which case a new ILPD record is automatically created) or matches an existing identity in the ILPD (in which case the identity information is linked to the existing ILPD record)
ILPD-5	Support discovery of providers by their attributes, including name, provider type, location, NPI, and Entity association
ILPD-6	Support representation of and discovery of the Entities with which a discovered provider is associated, as well as the retrieval of information describing these Entities

No.	CRITICAL FUNCTIONS
ILPD-7	Support access to all technical information needed to exchange information with a Provider in the context of a specific Entity. This information may include the provider's unique identifier and/or digital credentials specific to that Entity, as well as information about the Node(s) through which one may communicate with the Provider at that Entity, including the transactions and interoperability protocols that those Nodes support
ILPD-8	Support read-only access via a programmatic API, which implements (at a minimum) the Messaging and Authentication Frameworks described in this document
ILPD-9	Support read-only access via a web-browser interface and limit access to only other Providers registered in the ILPD
ILPD-10	Support write access via a programmatic API, which implements (at a minimum) the Messaging and Authentication Frameworks described in this document
ILPD-11	Support write access via a web-browser which will require two-factor authentication and be logged.
ILPD-10	Store two types of information about each licensed clinician: "Discoverable" attributes that describe the clinician sufficiently to unambiguously determine her identity when accessed by other Providers and Entities and "undiscoverable" attributes that include additional information needed to credential a clinician for purposes of health plan participation, clinical privileges, etc. These two types of information must be handled separately, so that the undiscoverable attributes are only disclosed at the direction and with the consent of the Provider, whereas discoverable attributes are available to any Provider or Entity with read access to the ILPD
ILPD-11	The ILPD records of licensed clinicians must include an X.509 class-3 digital certificate signed by Cal eConnect or a certificate authority designated by Cal eConnect. The ILPD records of unlicensed clinicians and non-clinician Providers may optionally include digital certificates, which may be signed by other certificate authorities as long as there is a chain of trust to Cal eConnect or its designated certificate authority
ILPD-12	The ILPD/ELPD mapping records of licensed clinicians whose identities are certified by the Entities that submitted them must include an X-509 class-3 digital certificate signed by the Entity
ILPD-13	Support distribution and federation of service instances to ensure acceptable performance and to allow local management within designated jurisdictions (e.g., states)
ILPD-14	Meet performance requirements
ILPD-15	All user-interface components shall be designed to maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.

No.	CRITICAL FUNCTIONS
ILPD-16	All APIs shall be designed to minimize the level of effort required on the part of California stakeholders and their H.I.T. vendors to integrate their solutions with the Cal eConnect infrastructure

7. *Cal eConnect Entity and Node*

In addition to the core services described above, Cal eConnect intends to also serve as an "Entity" and operate a Node that provides certain health information exchange capabilities for Providers who may not have access to Entities or Nodes. Every licensed Provider certified by Cal eConnect will be associated with the Cal eConnect Entity by default. This association will provide the ability to use the Cal eConnect Node for certain transactions to Providers. The functional and technical requirements of the Cal eConnect Entity (CE) and Cal eConnect Node (CN) are described below.

7.1. Functional Requirements

7.1.1. Provider/Entity Association

Providers shall be able to use their association with the Cal eConnect Entity to electronically request associations with other Entities. Upon valid two-factor authentication to the ILPD web-browser application, Providers shall be able to formulate and transmit requests to other Entities to be associated with them (see Section 6.1.4, Table 6.5). These requests shall be transmitted to the Entities using the Messaging and Authorization Frameworks described in this document and encoded in a formal message (payload) format that is to be determined. When Providers use the ILPD web-browser application to request association with an Entity, the request shall designate the Cal eConnect Entity as the sending Entity and shall include the digital certificate of the Cal eConnect Entity, as well as the digital certificate created by Cal eConnect for the Provider. The request shall also include an authentication assertion signed by the Cal eConnect Entity that verifies that a Provider authenticated to the ILPD using a two-factor method.

The interoperability protocol for submitting association requests from Providers to Entities shall be specified in the Services Registry under the transaction type "Provider_Request_For_Assocation". Providers will be able to request association with any Entity that uses a Node that supports this transaction and interoperability protocol (as documented in its ELPD Node record – see Section 3.2.1, Table 3.9 to Table 3.11). If a Provider attempts to use the ILPD to request an association with an Entity that does not use such a Node, the Provider will be informed that association with this Entity cannot be requested via the messaging standards and must be completed within the web based interactions supported by the Provider Directory web services.

7.1.2. Health Internet Service Provider

The Cal eConnect Entity and Cal eConnect Nodes shall serve as a Health Internet Service Provider (HISP) for Providers who have no associations with any other Entities or Nodes. These "unaffiliated providers" typically work in solo and small group practices of 5 or fewer MDs. These practices typically have limited I.T. resources to build and/or maintain data interfaces for their EHRs. To achieve interoperability with other enterprises (practices, labs, pharmacies, etc.) they typically rely on the intrinsic capabilities of their I.T. products and on the bundled services of their I.T. vendors. In the near term (1-3 years), unaffiliated providers will be challenged to achieve health information exchange even with the availability of the Cal eConnect Infrastructure, because these practitioners will lack the resources to interface their EHR systems to these services and to each other. In the longer term, it is anticipated that EHR vendors will incorporate connectivity with the Cal eConnect Infrastructure services into their products, as their customers (large and small practices alike) perceive the value of the services and the Messaging Framework as a means to communicate with each other and with other types of organizations (hospitals, labs, immunization registries, etc.)

Given this dynamic, an effective strategy for Cal eConnect to engage unaffiliated providers in the near term is to offer “bridging” technologies between EHRs and the Cal eConnect Infrastructure. These technologies have two key characteristics:

1. They are compatible with those capabilities of EHR systems that are required in stage-1 certification criteria or otherwise likely to exist in the near term, and
2. They enable the health information exchanges that are required under stage-1 meaningful use criteria.

The Cal eConnect Entity and Node shall provide HISP services in compliance with the specifications of the Direct Project *and* in compliance with the messaging and authorization frameworks defined in Section 1 and 2 of this document. The functions of the HISP shall be accessible to unaffiliated providers as both a web portal and (in the case of the Direct Project protocols) as an SMTP server.

The web-portal functionality shall include a secure “inbox” and “outbox” for health information exchange transactions, allowing the appropriate data files to be uploaded from or downloaded to the local file system as discrete files. It is likely that, under the stage-1 EHR certification criteria, EHRs will able to use the local file system for importing and exporting clinical summaries, immunization records, and ambulatory quality measures. In order to interface to the Cal eConnect Infrastructure and to the other organizations that use this infrastructure, the Cal eConnect Entity and Node will provide trusted authentication on behalf of unaffiliated providers, will create and maintain the provider’s entry in the ILPD/ELPD Mapping Database, and will enable providers to conduct the following transactions related to meaningful use:

- Secure exchange of clinical summaries with any other Provider who is able to use the Cal eConnect Infrastructure’s Messaging Framework and Authorization Framework *or* use the NwHIN Direct transport protocol (via a HISP or directly through their EHRs)
- Secure upload of an updated patient summary record to one of several untethered PHRs (Google, Microsoft, etc.) that is compatible with the Cal eConnect Infrastructure *or* the NwHIN Direct protocol
- Secure download of Lab Results from laboratories that are compatible with the Cal eConnect Infrastructure *or* the NwHIN Direct transport protocol
- Secure submission of immunization records to an appropriate immunization registry, and viewing or retrieval of immunization histories from the appropriate immunization registries (assuming the registry is compatible with the Cal eConnect Infrastructure *or* the NwHIN Direct transport protocol)
- Secure submission of ambulatory quality measures to CMS via the NHIN-gateway mechanisms that CMS is currently proposing.

Conducting these transactions via the Cal eConnect HISP will require practice personnel to import and export files between their EHR and their file system and certainly will not be as efficient as direct support by the EHR of the Messaging Framework and Authorization Framework. However, such a HISP service in conjunction with the services of the Cal eConnect Infrastructure, will prove very valuable for enabling unaffiliated providers to securely exchange health information with large ambulatory practices, hospitals, laboratories, and other participants prior to the time that these providers' EHR systems include built-in support for these frameworks. In addition, for those providers who have an EHR that can formulate messages consistent with the NwHIN Direct specifications, the Cal eConnect HISP can serve as a NwHIN Direct SMTP server.

7.1.3. Test Harness

As part of the development of the Cal eConnect Infrastructure, an application is needed to serve as a test harness for the ELPD, ILPD, Services Registry, Exchange Services, Messaging Framework, and Authorization Framework. Given its intended role as a HISP, the Cal eConnect Node can serve this purpose if it is implemented at an early stage in the development of the Cal eConnect Infrastructure. To fulfill the role as a test harness, the Cal eConnect Node should have the following features:

- Program logic, user interface, and API for submitting web-services calls to the ELPD and ILPD via the Messaging and Authorization Frameworks. This module should enable a user to view and validate the Entity, Provider, and Node information retrieved from these services and to use this information to formulate transactions consisted with the interoperability protocols listed in the Services Registry (e.g., sending a lab result or a patient visit summary). The module should also enable a user to create and modify entries in the ELPD and ILPD, as well as exercise all of the other functionalities of the core services.
- Program logic, user interface, and API for conducting transactions using the Messaging Framework and Authorization Framework. This module should enable a user to send or receive PHI in the form of a document transmitted as the payload of a message transmission. The module should also generate the appropriate authorization artifacts to conduct these transactions, as well as verify authorization artifacts sent by counterparties.
- For demonstration purposes, the application should be available as a web-based portal that can be accessed remotely. The application should have a small number of sample document available (such as lab results, discharge summaries, ambulatory patient summaries, and immunization events), as well as a viewer for these document types.

7.1.4. Compatibility Testing Tool

The Cal eConnect Entity and Node should also serve as a testing tool for developers who are building their own Nodes for conducting HIE transactions. Specifically, the Cal eConnect Node should provide a web service that enables the developers of HIE Nodes in California to test whether their implementations of standard interoperability protocols are correct (i.e., the protocols listed in the Services Registry – see Section 4). This web service will analyze test messages generated and sent by an arbitrary Node to determine whether the messages are compliant with the intended interoperability protocol. The web service will also generate and send test messages to an arbitrary Node to determine whether the Node can correctly receive, parse, and process messages that are compliant with the intended interoperability protocol. The service will assist the developers of Nodes to verify that their implementations are compliant with the standard protocols that they wish to list in their ELPD entries. When the developers of Nodes have successfully completed such testing, they will be entitled to assert within the ELPD record for their Nodes that the Nodes are compliant with the tested interoperability protocols. It is envisioned that this use of the service will be voluntary.

The web service will also enable Cal eConnect, itself, to periodically verify that Nodes registered in the ELPD remain active and able to process the transactions and interoperability protocols they claim to support. All Nodes registered in the ELPD will be required to accept these "ping" messages issued by Cal eConnect for each of the interoperability protocols they support, and return a suitable acknowledgement that includes sufficient information to verify that the test message was received and correctly interpreted. The specifications for processing such "ping" messages will be included in the definitions of the interoperability protocols.

7.2. Technical Requirement

The Cal eConnect Node shall be implemented as a web portal accessible via standard modern web browsers using commonly supported protocols for transport-level security, including:

- Apple Safari V4/V5 supporting TLS V1.0
- Firefox supporting TLS V1.0
- Internet Explorer 8 in Windows 7 supporting TLS V1.2
- Presto 2.2 and Opera 10 supporting TLS V1.2

The Cal eConnect Node shall require all users to be certified and registered in the ILPD and shall use two-factor authentication to validate the identity of these users when they log into the Node.

The Cal eConnect Node shall implement the transport and security models of the Messaging Framework and Authorization Framework, as described in Sections 1 and 2. It shall also serve as a "client" application with respect to the other services of the Cal eConnect Infrastructure, specifically implementing all of the API calls listed in Sections 3, 4, 5, 6, and 7.

The Cal eConnect Node shall provide a high level of security that is impervious to malicious break-in, spoofing and denial-of-service attacks launched from the public internet.

7.3. Usability Requirements

All user-interface components shall be designed to maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.

7.4. Critical Functions of Solution

The responding Bidder may propose variations to the specifications described above as long as the Bidder's specifications are functionality equivalent. The critical functions that must be met by the vendor's proposed solution are listed in Table 7.1.

Table 7.1. Critical functions of the solution for the Cal eConnect Entity and Node

NO.	CRITICAL FUNCTIONS
CEN-1	Support the Messaging and Authorization Frameworks
CEN-2	Support the set of transactions for the Direct transport protocol
CEN-3	Provide a Web service that can evaluate inbound test messages submitted by developers to determine compliance with the standard interoperability protocols defined by Cal eConnect, as well as generate outbound test messages for developers to determine whether their implementations can correctly process messages compliant with the standard interoperability protocols defined by Cal eConnect
CEN-4	Provide a highly secure web-browser application that can be accessed by licensed clinicians registered in the ILPD
CEN-5	Implement two-factor authentication for access to the web-browser application
CEN-6	Provide performance and response times compatible with synchronous use by Providers
CEN-7	Design all user-interface components to maximize usability by the intended audiences, including the design of intuitive work flow, appropriate terminology, online help features, etc.

Table 7.2. Critical functions of the solution for the Cal eConnect Test Harness

No.	CRITICAL FUNCTIONS
TF-1	Provide a web based service for a Node to test its ability to correctly utilize the messaging framework and each of the API (methods) available to the Node from the Provider Directory Services
TF-2	Provide a web based service for a Node to test its ability to formulate and send an SR compliant message in any of the messaging frameworks (Cal eConnect, Direct Project and NwHIN Exchange) and provide feedback to the testing node on inconsistent message structure where possible
TF-3	Provide a web based service for a Node to test its ability to formulate and send an SR compliant payload (e.g. CCD C32, or HL7 2.5.1 ELINCS, LOINC) and provide feedback to the testing node on inconsistent payload structure where possible

No.	CRITICAL FUNCTIONS
TF-4	Provide a web based service that emulates a sending Node to allow a receiving node to test its ability to receive and consume SR compliant payloads (e.g. CCD C32, or HL7 2.5.1 ELINCS, LOINC)

EXHIBIT C – CAL ECONNECT'S PMO QUALITY ASSURANCE SURVEILLANCE PLAN

1. Purpose

Cal eConnect's PMO Quality Assurance Surveillance Plan provides procedures and guidelines that the Cal eConnect PMO will use in evaluating Contractor performance. The PMO QA Surveillance Plan will be given to the Contractor during the project initiation phase to ensure understanding specific to how performance will be evaluated. The Surveillance/Evaluation Methods outlined in the QASP, in concert with the Contractor's Quality Control Procedures (QCP), will assure satisfactory performance.

The QASP is intended to accomplish the following:

- Clearly define work to be performed and required results
- Clearly describe the evaluation methods used by Cal eConnect's PMO in assessing the Contractor's performance
- Define the process for documenting performance

The QASP is one tool used by the PMO to manage contract, but is subject to revisions throughout the contract performance period. Cal eConnect will retain the right to change the surveillance methods, metrics and Quality Assurance (QA) procedures described in the plan, or to increase or decrease the degree of surveillance efforts at any time necessary to assure contract compliance. Cal eConnect will work in collaboration with the Contractor to modify, as needed, changes to Quality Control Procedures (QCP).

The Contractor is responsible for management and implementation quality control procedures to meet the terms of the contract.

2. Surveillance Procedures

2.1. Performing Surveillance

Surveillance will be conducted as outlined in the QASP. Surveillance includes scheduling, observing, documenting, and resolving performance issues discovered through surveillance procedures. Even though Cal eConnect will be monitoring the Contractor's performance on a continuing basis, the volume of tasks performed by the Contractor makes technical inspections of every task and step impractical. Accordingly, only some tasks will be listed as monitored and evaluated as specified in the Performance Requirements Summary.

2.2. Surveillance Approach

Cal eConnect's PMO surveillance strategy is oversight and evaluation of performance requirements as set forth in the Statement of Work. Performance requirements and metrics will be used to ensure process capability, product quality and delivery and end-item effectiveness. A minimum set of product or process data that provides adequate visibility into the integrity of the product or process will be gathered. The data may be acquired from Contractor records/reports, usually in a non-intrusive parallel method.

2.3. Documenting Surveillance

Documentation is required to record, evaluate, and report Contractor's performance. This documentation provides the PMO with Contractor status as it applies to the performance criteria. The PMO is required to maintain accurate records of the Contractor's performance and documenting surveillance. All documentation resulting from surveillance must be made part of the contract file.

2.4. Monthly Performance Meetings

PMO personnel, Contractor (or representative), and other Cal eConnect project-related personnel will meet monthly at Monthly Performance Meetings to discuss contract performance, resolve issues, discuss customer complaints, and provide positive interaction and feedback to all parties. The PMO will provide a list of any unresolved deficiencies to the Contractor's quality assurance representative to afford him/her the opportunity to demonstrate the issue is being addressed. If evidence is shown where the Contractor's quality program has already documented the deficiency and timely corrective action is taken to resolve the issue, the Lead Project Manager for the PMO will follow up with the Contractor's quality control representative to ensure the deficiencies are remedied in a timely manner, in accordance with the SOW. All deficiencies associated with performance requirements listed on the Performance Requirements Summary, whether remedied by the Contractor or not, will be included in the PMO's Monthly Report regardless of who identified the deficiency. A copy of the meeting minutes will be provided to all attendees within 5 workdays of the meeting. Monthly Performance Meetings will be scheduled between the time the Contractor submits the monthly Status Reports and its invoice.

3. Surveillance Methods

Performance evaluation will be accomplished by monitoring compliance with the performance requirements as described in the contract and in the following section of this QASP. The method of evaluation will depend on the service type, and each service type may be assessed by more than one method. The following evaluation methods will be used on the Provider Directory Services with eHIE Capabilities contract:

- Periodic Inspection – Evaluates tasks selected on other than a 100% or random basis. It may be appropriate for tasks that occur infrequently and where 100% inspection is neither required nor practicable.
- Independent Verification and validation (IV&V) – Verification and validation will be performed by an individual or organization that is technically, managerially, and financially independent of the development organization. The IV & V will be used to determine that technical work products delivered by the Contractor meet contract requirements. This may include various types of system tests, analysis or other V&V techniques.

The mapping of specific surveillance methods to performance requirements are provided below. The method of surveillance is a function of the activities being monitored and associated performance measures.

Once a month or as required by the performance requirement (frequency will be dependent on the specific performance requirement), the Lead Project Manager will review documentation and/or observe accomplishment of Performance Requirement(s) to ensure the minimum

Performance Standard(s) has (have) been met for the respective Performance Requirement(s). All performance must be documented, whether it is acceptable or unacceptable.

4. Performance Requirements

4.1. General Acceptance Criteria

As stated in the Cal eConnect Core Services Scope of Work, the following general quality measures, as set forth below, shall be applied to each work product received from the Contractor under this Contract. All deliverable products shall be evaluated for acceptance using the following general criteria in addition to other deliverable specific acceptance criteria.

- Accuracy – Work Products shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity – Work Products shall be clear and concise. Any/all diagrams shall be easy to understand and be relevant to the supporting narrative.
- Consistency with Requirements – All work products must satisfy the requirements of this SOW.
- File Editing – All text and diagrammatic files shall be editable by the Cal eConnect.
- Format – Work Products shall be submitted in hard copy (where applicable) and in media mutually agreed upon prior to submission. Hard copy formats shall follow any specified Directives or Manuals.
- Timeliness – Work Products shall be submitted on or before the due date specified or submitted in accordance with a later scheduled date determined by the Cal eConnect.

4.2 Specific Acceptance Criteria for Written Deliverables

The following specific criteria will be used when evaluating specific written deliverables listed in Section III, Scope of Work.

Deliverable: Project and Management Plan

Description: The Project and Management Plan specifies the tasks, sub tasks, and approaches to be used to provide the services and products required to satisfy Contract requirements including deliverable documents, analyses, and reports.

Acceptance Criteria: The Project and Management Plan shall include the following:

- Project Plan – The Project Plan shall be developed in Microsoft Project and must include tasks representing the Work Breakdown Structure (WBS) required for the Contractor to successfully complete the tasks given in this statement of work. Task dependencies and dates, resource loading, updated milestone and deliverable dates shall be included.
- Management Approach – The Management Approach shall be a Microsoft Word formatted document that describes the organizational resources and management controls employed to meet cost, performance, and schedule requirements as outlined in the project schedule. This shall detail the products, methods for producing deliverables, allocation of staff and other resources necessary to produce deliverables, and timelines, and any Furnished Information/Equipment expected from Cal eConnect (FI/E). A risk management plan shall be included that outlines project risks, potential severity of those risks, and mitigation strategies for those risks.

Acceptable Project and Management Plans will include the above information, in the formats requested, and in sufficient detail to cover all tasks.

Deliverable: Contract Budget Tracking Report

Description: Weekly, monthly, and on demand budget status reports.

Acceptance Criteria: The Contract Budget tracking process and resulting reports must be capable of providing weekly, monthly, and on demand budget status reports.

- Process involves the use of tools that facilitate the tracking and reporting of budget status, such as Microsoft Office products including Microsoft Access and Microsoft Excel.
- Process is capable of providing weekly, monthly, and on demand budget status reports.
- Process and associated reports is delivered not later than 30 days after award of the contract or as approved in the final Cal eConnect approved Contractor provided Project and Management Plan.

Deliverable: Weekly Project Status and Progress Review

Description: The Weekly Project Status and Progress Review Report is a management meeting between the Cal eConnect PMO and the Contractor to discuss project status.

Acceptance Criteria: The weekly status report shall be delivered on schedule and contain all required information. Information shall be current, accurate, and complete. As a minimum, the report shall contain the following.

- Activities planned for the week
- Work and deliverables completed during the week
- Status of ongoing activities
- Activities planned for the following week
- Problems or issues projected or identified
- Alternatives and/or recommended solution(s) for identified or projected problems or issues
- Known or projected resource (staff and funding) and schedule impacts

Deliverable: Monthly Project Status and Progress Summary Report

Description: The Monthly Project Status and Progress Summary Review shall be comprised of weekly management issues and include sufficient detail to ensure understanding of task progress and issues. The final deliverable must be suitable for forwarding to Cal eConnect executive management.

Acceptance Criteria: The monthly status report shall be delivered on schedule and contain all required information. Information shall be current, accurate, and complete. As a minimum, the report shall contain the following:

- Program status including objectives met and outstanding;
- Activities planned for the reporting period;
- Work and deliverables completed during reporting period;
- Status of ongoing activities including percentage of completion;
- Status of deliverables and/or milestones;
- Activities planned for the following reporting period;
- Planned travel during the following reporting period;
- Problems or issues projected or identified;
- Alternatives and/or recommended solution(s); i.e., risk mitigation strategy, for identified or projected problems or issues;
- Known or projected resources (staff and funding) and schedule impacts; and
- Status of project funds including monthly and total expenditures and funds remaining.
- Special topics or issues identified or requested by the Project Manager.

Deliverable: Monthly Financial Management Status Report

Description: The Monthly Financial Management Status Report provides current financial and resource utilization information for management review and decision making.

Acceptance Criteria: Data and information shall be broken out by major activity and include subtotal and total information as well as detailed data. The report shall be delivered to the PMO on schedule and contain all required information. Information shall be current, accurate, and complete. The delivered Report must be of suitable quality and presentation for forwarding to Cal eConnect executive management. The format and content of the Report shall include the following as a minimum:

- Budgeted total and budgeted monthly hours by major activity and Contract total.
- Actual hours expended for the reporting period by unit including breakdown by labor category and name for each major activity and the Contract total.
- Actual hours expended to date by task including breakdown by labor category and name including task totals, major activity totals, and Contract total

- Actual costs to date and for the reporting period (based on actual hours) by major activity and Contract total.
- Estimated Cost to Completion by major activity and Contract total.
- Estimated Cost at Completion by major activity and Contract total.
- Task and cost variance (for >10% variance include explanation/analysis) by major activity and Contract total.

Deliverable: Performance Based Services Plan

Description: The Performance Based Services Plan (PBSP) defines in detail the methods and procedures to be used to implement and perform tasks under a performance based contract.

Acceptance Criteria: The PBSP shall include, but is not limited to, the following in sufficient detail to allow implementation, tracking, reporting, and administration of the performance based services and incentives.

- Performance Monitoring: The purpose of performance monitoring and the proposed monitoring methods to be used with descriptions and evaluation tools or instruments to be used.
- Data Collection and Processing: The proposed methodologies and tools or instruments to be used for collection, analysis, and reporting of performance metrics, trends, status, and results.
- Performance Reporting: The proposed reporting schedules, report format and contents, and performance indicators, summaries, and comparisons to be used.
- Performance Award Administration: Proposed fee or payment withholding percentages, positive and negative performance incentives to be applies, and the review process to be followed to determine incentive application.
- Change Management of the Performance Based Services Plan: The proposed approach to PBSP modification to reflect changed operational and/or program priorities.

Deliverable: Other Deliverables

Description: Other deliverable products within scope of the Contract and required to provide services and perform tasks specified in the SOW.

Acceptance Criteria: Other deliverables shall be submitted in formats and evaluated according to criteria agreed upon by the Contractor and the Cal eConnect PMO.

4.3. Performance Summary for Other than Written Deliverables

Performance Requirement	Performance Standard	Monitoring Method
Hosting and Security		
Entity Level Provider Directory Performance Requirements	Response time per read operation: < 1 second	Inspection of system monitoring reports produced by Contractor
	Response time per write operation: < 5 seconds	Inspection of system monitoring reports produced by Contractor
	Availability for read and write operations: 99.999% 24x7x365	Inspection of system monitoring reports produced by Contractor
Services Registry Performance Requirements	Response time for write operations: < 3 second	Inspection of system monitoring reports produced by Contractor
Individual Level Provider Directory Performance Requirements	Response time – Provider search operation: < 3 second	Inspection of system monitoring reports produced by Contractor
	Response time – Provider record retrieval operation: < 1 second	Inspection of system monitoring reports produced by Contractor
	Response time – Provider Entity retrieval operation: < 1 second	Inspection of system monitoring reports produced by Contractor
	Response time – Provider Node retrieval operation: < 1 second	Inspection of system monitoring reports produced by Contractor
	Response time for all write operations (API or web browser): < 3 seconds	Inspection of system monitoring reports produced by Contractor
	Availability for read and write operations: 99.999% 24x7x365	Inspection of system monitoring reports produced by Contractor
Call Center and Data Trading Partner Support		
Call Answering Performance Requirements	90% of calls answered in 4 rings or less	Analysis of help desk escalations and end-user feedback.
	Average time on hold less than 4 minutes	Analysis of help desk escalations and end-user feedback.
	Less than 5% of calls receive busy signal	Analysis of help desk escalations and end-user feedback.
Help Desk Response	98% of Priority 1 calls	Analysis of help desk

Performance Requirement	Performance Standard	Monitoring Method
Performance Requirements (per Help Desk Response Targets in the table below)	resolved in less than one day	escalations and end-user feedback.
	98% of Priority 2 calls resolved in less than three days	Analysis of help desk escalations and end-user feedback.
	98% of Priority 3 calls resolved in less than five days	Analysis of help desk escalations and end-user feedback.
	98% of Priority 4 calls resolved in less than 20 days	Analysis of help desk escalations and end-user feedback.

Help Desk Response Targets

Priority	Criteria	Target Response Time
1	Affects more than five individuals (whether in a single Entity or in multiple Entities); or is mission critical and there is no workaround available.	Immediate response.
2	Affects one to five individuals (whether in a single Entity or in multiple Entities), no workaround available.	Initial response within 4 working hours.
3	Affects fewer than five people (whether in a single Entity or in multiple Entities), workarounds available.	Initial response within one working day.
4	No effect on productivity.	Best effort as time allows.

EXHIBIT D – HEALTH INFORMATION EXCHANGE USE CASES / SCENARIOS AND RELATED QUESTIONS FOR BIDDERS

1. Introduction

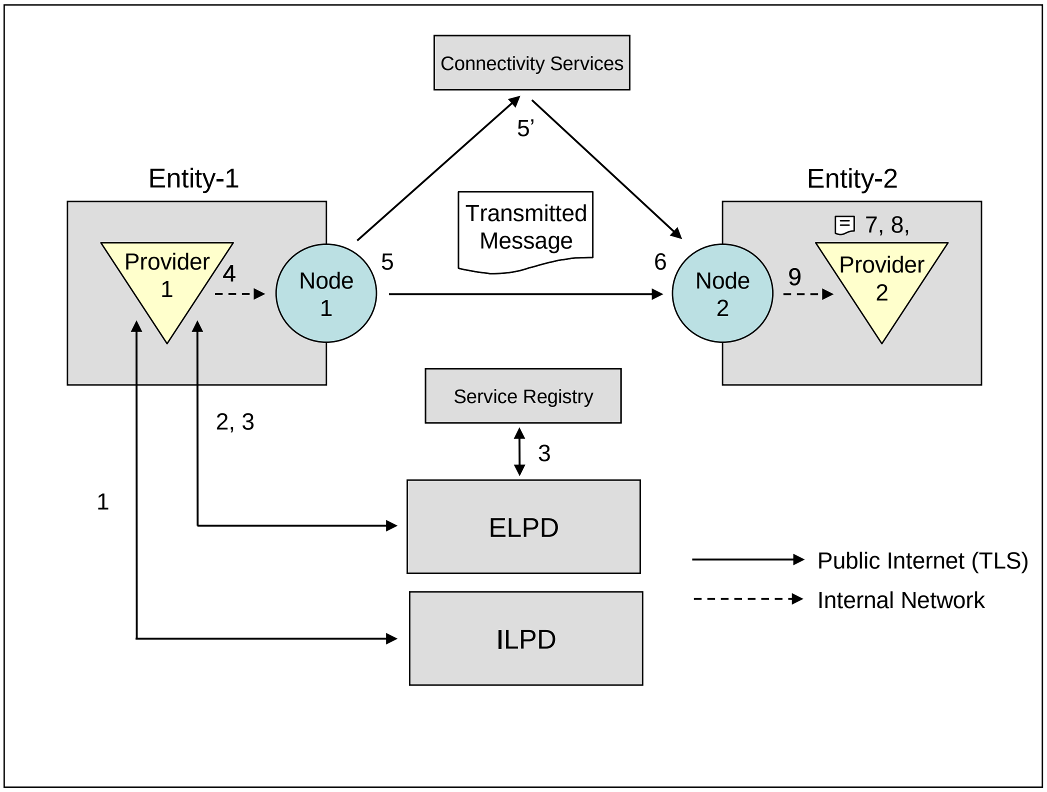
This exhibit includes seven health information exchange scenarios (referred to as “use cases” below), each describing a different workflow enabled by the use of the messaging framework, provider directory, and exchange services infrastructure. Each use case is followed by several questions, the answers to which will be used to validate the vendor’s understanding of the scenarios and requirements, while evaluating the completeness of the proposed solution. The first six use cases are intended to validate the provider directory services with eHIE capabilities infrastructure architecture. The seventh use case is intended to collect information regarding the business operations of Cal eConnect.

The overview below describes how senders and recipients will use the provider directory services with eHIE capabilities infrastructure to complete transactions. See Exhibit B for the detailed provider directory services with eHIE capabilities infrastructure requirements and specifications. The information in that exhibit will be helpful in understanding the use cases and answering the questions below.

2. Overview of Provider Directory Services with eHIE Capability Infrastructure Transactions

The infrastructure is intended to support the discovery of certified Individuals and Entities along with their registered Nodes, security artifacts and clinical messaging standards; with the goal of enabling secure communications that are trusted by both the senders and recipients of health information transactions. Figure D.1 illustrates how the components of the infrastructure enable the sender and the recipient of a message to validate its destination and source (respectively). The description below this figure describes the steps involved. In this example, the sender is Provider-1, who is associated with Entity-1 and uses Node-1 for transactions. The recipient is Provider-2, who is associated with Entity-2 and uses Node-2 for transactions.

Figure D.1 Use of infrastructure components for secure and trusted messaging



<u>Sender (Provider-1):</u>

1. **Query Individual Provider Directory:** Provider-1 accesses the ILPD and searches for the provider record of the intended recipient. This record enables the sender to confirm the identity of the recipient by inspecting the recipient provider's demographic attributes, National Provider Identifier, specialty, practice affiliation, etc. Each licensed provider record in this directory includes a digital certificate, which specifies the Provider's certified identity and public key. The digital certificates for licensed providers may be issued by Cal eConnect or by the Provider's Entity. The ILPD also contains links between the Provider and the Entities with which she is associated.

2. **Query Provider's Associated Entity:** Provider-1 accesses the ELPD to retrieve information about the specific Entity relevant for the intended transaction (e.g., the recipient's hospital versus the recipient's outpatient practice). The Entity record includes a digital certificate issued by or on behalf of Cal eConnect certifying the Entity's identity and public key. The Entity record also includes a link to the Node records that describe the technical capabilities of the Entity for receiving and sending health information transactions.

3. **Query Entity's Node Record and Services Information:** Provider-1 retrieves the Node record, which includes the Node's digital certificate. The Node record also lists (1) the specific types of transactions that the Node supports (e.g., send patient summary, send lab result, etc.), (2) the specific electronic address at which it supports each transaction, and (3) the specific interoperability protocols it supports for each transaction. The ELPD retrieves the detailed specifications for these interoperability protocols from the Services Registry (such as "HL7 v2.5.1 with ELINCS Implementation Guide and LOINC test

coding"). This transaction, addressing, and protocol information about the Node enables the provider's I.T. system to correctly formulate the intended transaction for the intended recipient. The digital certificates within the Provider's, Entity's, and Node's records establish a chain of trust between Cal eConnect and the recipient Provider, Entity, and Node.

4. **Encrypt Payload:** The sending provider's EHR or (as appropriate) the designated intermediary for the provider encrypts the payload containing the PHI using the recipient provider's public key.

5. **Request Trusted Connection:** Before transmission of the health information to the published address, the Node at that address is validated by inspecting its digital certificate and signature as part of the TLS handshake.

5'. **Utilize Exchange Services:** If necessary, the sending Node alternatively uses the Exchange Services as a "proxy" to translate the interoperability protocol that it uses to one that the receiving node can process.

Recipient (Provider-2):

6. **Accept Trusted Connection:** The receiving Node validates the sending Node by inspecting its digital certificate and signature as part of the TLS handshake.

7. **Verify sending Entity certificate:** The receiving Node inspects the digital certificate of the sending Entity (included in the message) and validates it as a legitimate Entity (i.e., by virtue of having a certificate signed by Cal eConnect).

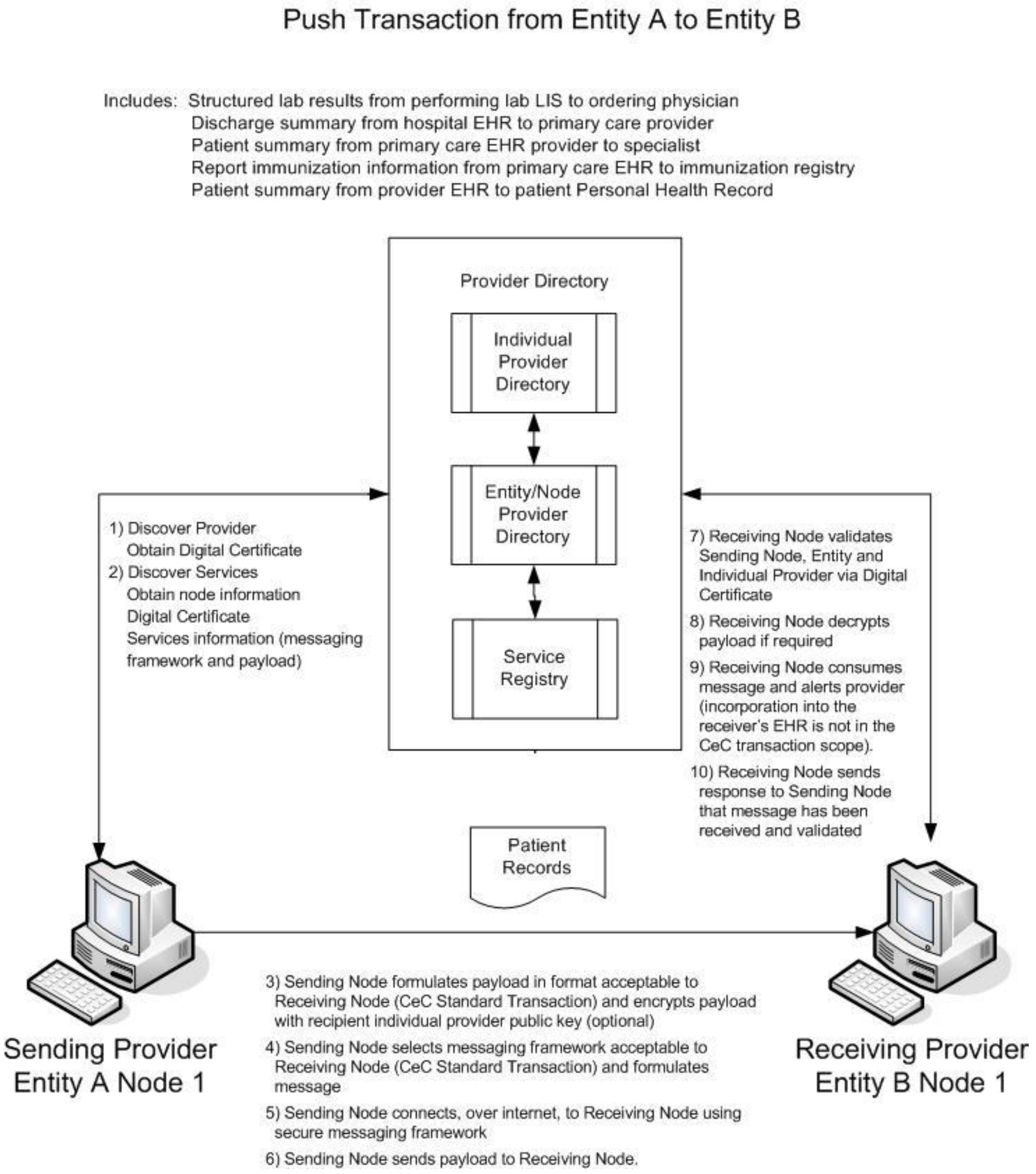
7. **Confirm Sending Entity:** The message signature is validated to have been generated by the sending Entity, confirming origination at that Entity (i.e., non-repudiation of source).

8. **Confirm Sending Provider:** The digital certificate for the sending Provider is inspected and validated, as well as the authentication assertion that was digitally signed by the sending Entity (verifying that the Provider properly authenticated). The Provider's digital certificate, the Entity's digital certificate, and the signed authentication assertion establish a chain of trust between Cal eConnect and the sending Provider and validate that the message originated from this provider.

9. **Decrypt Payload:** The receiving provider's EHR or (as appropriate) the designated intermediary for the provider decrypts the payload containing the PHI using their private key.

3. *Use Case 1: Push Transaction -- Hospital Discharge Summary to Clinician*

General Push Transaction:



Push Transaction from Entity A to Entity B

Includes: Structured lab results from performing lab LIS to ordering physician
Discharge summary from hospital EHR to primary care provider
Patient summary from primary care EHR provider to specialist
Report immunization information from primary care EHR to immunization registry
Patient summary from provider EHR to patient Personal Health Record

Provider Directory
Individual Provider Directory
Entity/Node Provider Directory
Service Registry
Patient Records
Sending Provider Entity A Node 1
Receiving Provider Entity B Node 1

1) Discover Provider
Obtain Digital Certificate

2) Discover Services
Obtain node information
Digital Certificate
Services information (messaging framework and payload)

3) Sending Node formulates payload in format acceptable to Receiving Node (CeC Standard Transaction) and encrypts payload with recipient individual provider public key (optional)

4) Sending Node selects messaging framework acceptable to Receiving Node (CeC Standard Transaction) and formulates message

5) Sending Node connects, over internet, to Receiving Node using secure messaging framework

6) Sending Node sends payload to Receiving Node.

7) Receiving Node validates Sending Node, Entity and Individual Provider via Digital Certificate

8) Receiving Node decrypts payload if required

9) Receiving Node consumes message and alerts provider (incorporation into the receiver's EHR is not in the CeC transaction scope).

10) Receiving Node sends response to Sending Node that message has been received and validated

Typical Story

A hospital discharge summary is sent from a hospital EHR to a primary care physician's EHR at the relevant practice location. The physician’s EHR system receives the discharge summary and incorporates data from it into the patient's electronic record.

Provider Directory and Trust Framework Steps (elaboration on certain steps from Section 2)

1 **Query Individual Provider Directory** – Sending Provider at the hospital queries for the desired outpatient Provider to receive the discharge summary.

Query Provider’s Associated Entities – selects the appropriate entity/location where the patient receives primary care and where the patient’s electronic record is maintained.

2 **Query Entity’s Node Record and Services Information** – selects the Node to receive the information and determines the supported protocols and payloads for the receipt of a discharge summary.

7 **Verify Sending Entity Certificate** – physician’s EHR verifies the sending entity is trusted by Cal eConnect.

7 **Confirm Sending Entity** – physician’s EHR verifies the message is signed by the trusted entity

8 **Confirm Sending Provider** – physician’s EHR verifies the identity of the sending provider (in this case the responsible physician at the hospital)

Provider Directory Entries:

ILPD	Providers (physicians, nurse practitioners, physician assistants), Departments
ELPD	Entities (hospitals, physician practices, clinics …) and Nodes for each

Services Registry: Supported protocols and payloads for each transaction type

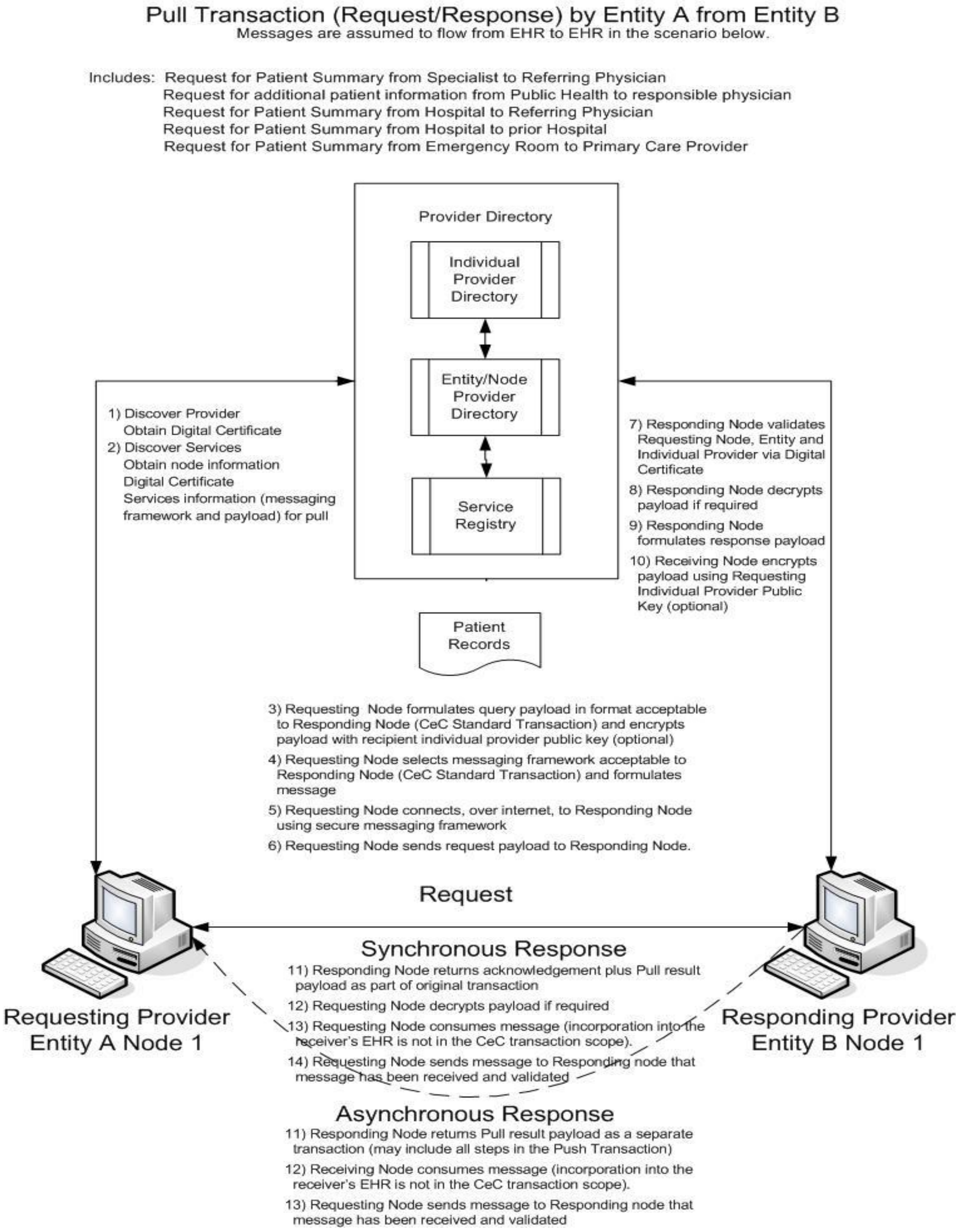
Questions:

1. Describe in detail how your proposed solution will meet the requirements for this use case. Please list all assumptions.
2. Describe which capabilities currently exist in your solution and which will need to be developed
3. Describe the current capability of your solution to support multiple messaging standards. At a minimum describe you support for NwHIN Exchange, Direct Project, and the ability to create and support the framework described in Exhibit B (used by EHRs to communicate with the Provider Directory Services, the Exchange Services, and between each other) .
4. Describe the security and authorization artifacts and message types that will be needed by your solution to support the Push transaction.

5. If a specific Sending EHR or Receiving EHR does not support any of the messaging frameworks (NwHIN Exchange, Direct Project, or Cal eConnect Messaging Framework) how will your solution support the communication of patient information between these EHRs?
6. Please list all Immunization registries and departments of public health with which your solution currently exchanges information electronically and the protocols it supports to do so.
7. Since one of the possible uses of these transactions is communication with health plans to enable various X.12 transactions, please list the health plans with which your solution currently exchanges information in an X.12 format and the specific X.12 transactions supported

4. Use Case 2: Pull Transaction – Patient Summary request by Specialist

General Pull Transaction:



Pull Transaction (Request/Response) by Entity A from Entity B

Messages are assumed to flow from EHR to EHR in the scenario below.

Includes: Request for Patient Summary from Specialist to Referring Physician
Request for additional patient information from Public Health to responsible physician
Request for Patient Summary from Hospital to Referring Physician
Request for Patient Summary from Hospital to prior Hospital
Request for Patient Summary from Emergency Room to Primary Care Provider

Provider Directory
Individual Provider Directory
Entity/Node Provider Directory
Service Registry
Patient Records
Request
Requesting Provider Entity A Node 1
Responding Provider Entity B Node 1

1) Discover Provider
Obtain Digital Certificate

2) Discover Services
Obtain node information
Digital Certificate
Services information (messaging framework and payload) for pull

7) Responding Node validates Requesting Node, Entity and Individual Provider via Digital Certificate

8) Responding Node decrypts payload if required

9) Responding Node formulates response payload

10) Receiving Node encrypts payload using Requesting Individual Provider Public Key (optional)

3) Requesting Node formulates query payload in format acceptable to Responding Node (CeC Standard Transaction) and encrypts payload with recipient individual provider public key (optional)

4) Requesting Node selects messaging framework acceptable to Responding Node (CeC Standard Transaction) and formulates message

5) Requesting Node connects, over internet, to Responding Node using secure messaging framework

6) Requesting Node sends request payload to Responding Node.

Synchronous Response

11) Responding Node returns acknowledgement plus Pull result payload as part of original transaction

12) Requesting Node decrypts payload if required

13) Requesting Node consumes message (incorporation into the receiver's EHR is not in the CeC transaction scope).

14) Requesting Node sends message to Responding node that message has been received and validated

Asynchronous Response

11) Responding Node returns Pull result payload as a separate transaction (may include all steps in the Push Transaction)

12) Receiving Node consumes message (incorporation into the receiver's EHR is not in the CeC transaction scope).

13) Requesting Node sends message to Responding node that message has been received and validated

Typical Story

A specialist requests a patient summary from a referring physician. In response, the referring physician EHR sends a patient summary to the specialist, either synchronously or asynchronously. The specialist's EHR system receives the patient summary and incorporates data from it into the patient's record.

Provider Directory and Trust Framework Steps (elaboration on certain steps from Section 2)

1 **Query Individual Provider Directory** – Requesting Provider queries for the desired referring Provider to obtain the patient summary.

Query Provider's Associated Entities – selects the appropriate entity/location where the patient receives primary care and where the patient's electronic record is maintained.

2 **Query Entity's Node Record and Services Information** – selects the Node to receive the information and determines the supported protocols and payloads for the transmission of a patient summary.

7 **Verify Requesting Entity Certificate** – physician's EHR verifies the requesting Entity is trusted by Cal eConnect.

7 **Confirm Requesting Entity** – primary care physician's EHR verifies the message is signed by the trusted entity

8 **Confirm Requesting Provider** – primary care physician's EHR verifies identity of the requesting provider (in this case the requesting specialist)

Provider Directory Entries:

ILPD	Providers (physicians, nurse practitioners, physician assistants), Departments
ELPD	Entities (hospitals, physician practices, clinics …) and Nodes for each

Services Registry: Supported protocols and payloads for each transaction type

Questions:

1 Describe in detail how your proposed solution will meet the requirements for this use case. Please list all assumptions.

2 Describe which capabilities currently exist in your solution and which will need to be developed

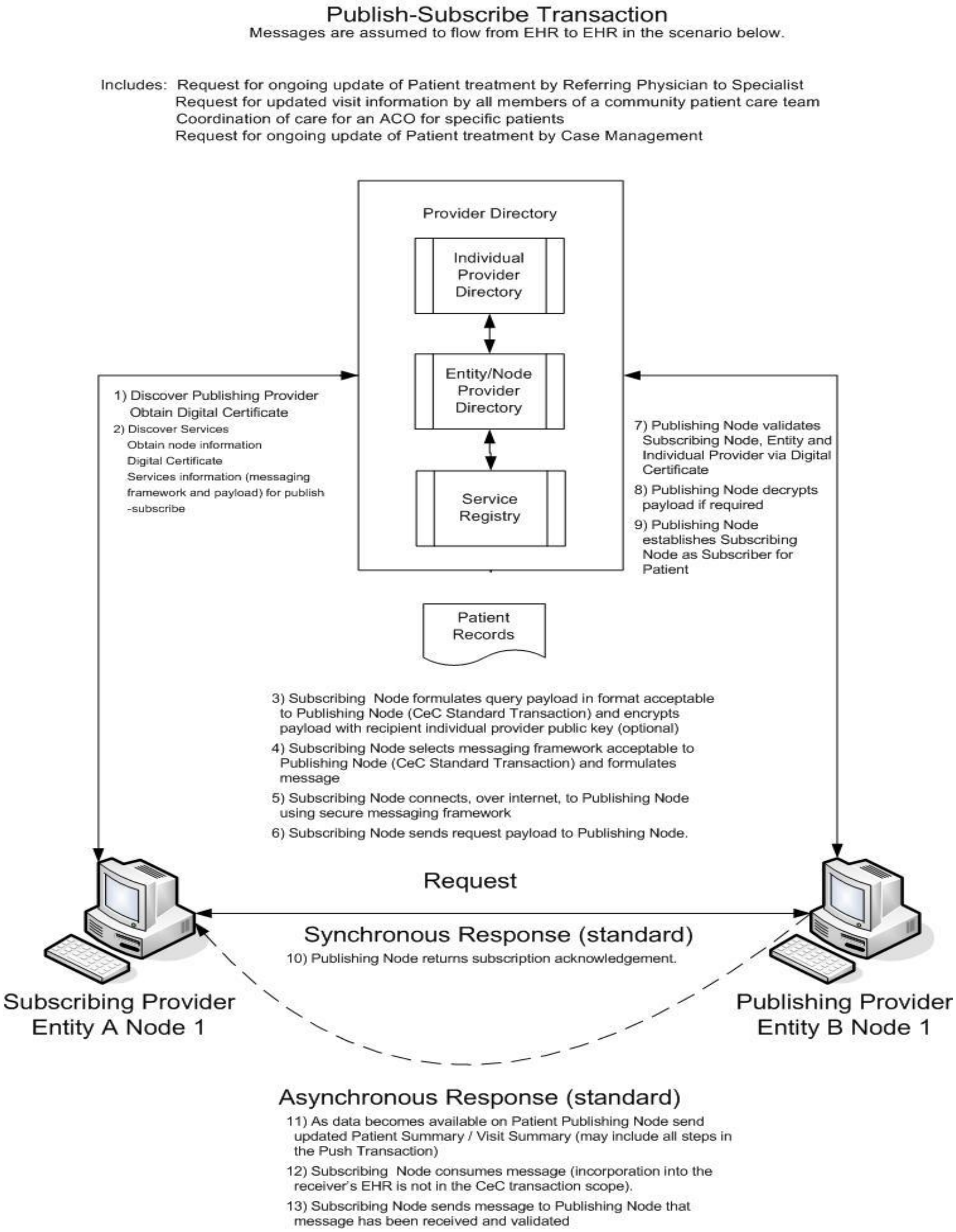
3 Describe the current capability of your solution to support multiple messaging standards that allow a "Pull" transaction. At a minimum describe you support for NwHIN Exchange, Direct Project, and the ability to create and support the framework described in Exhibit B.

4 Describe the additional artifacts and message types that will be needed by your solution to support the Pull transaction.

5 If a specific Sending EHR or Receiving EHR does not support a Pull transaction how do you propose that the requester and sender communicate the requested patient information?

5. *Use Case 3: Publish-Subscribe Transaction – Request by referring Physician to Specialist for ongoing updates of Patient Treatment*

General Publish-Subscribe Transaction:


Publish-Subscribe Transaction
Messages are assumed to flow from EHR to EHR in the scenario below.
Provider Directory
Individual Provider Directory
Entity/Node Provider Directory
Service Registry
Patient Records
Request
Synchronous Response (standard)
Subscribing Provider Entity A Node 1
Publishing Provider Entity B Node 1
Asynchronous Response (standard)

Includes: Request for ongoing update of Patient treatment by Referring Physician to Specialist
Request for updated visit information by all members of a community patient care team
Coordination of care for an ACO for specific patients
Request for ongoing update of Patient treatment by Case Management

1) Discover Publishing Provider
Obtain Digital Certificate

2) Discover Services
Obtain node information
Digital Certificate
Services information (messaging framework and payload) for publish -subscribe

3) Subscribing Node formulates query payload in format acceptable to Publishing Node (CeC Standard Transaction) and encrypts payload with recipient individual provider public key (optional)

4) Subscribing Node selects messaging framework acceptable to Publishing Node (CeC Standard Transaction) and formulates message

5) Subscribing Node connects, over internet, to Publishing Node using secure messaging framework

6) Subscribing Node sends request payload to Publishing Node.

7) Publishing Node validates Subscribing Node, Entity and Individual Provider via Digital Certificate

8) Publishing Node decrypts payload if required

9) Publishing Node establishes Subscribing Node as Subscriber for Patient

10) Publishing Node returns subscription acknowledgement.

11) As data becomes available on Patient Publishing Node send updated Patient Summary / Visit Summary (may include all steps in the Push Transaction)

12) Subscribing Node consumes message (incorporation into the receiver's EHR is not in the CeC transaction scope).

13) Subscribing Node sends message to Publishing Node that message has been received and validated

Typical Story

A referring primary care physician requests the consulting specialist to send ongoing updates of the patient's treatment as visits occur over time. In response, the specialist's EHR records the request and sends visit / treatment updates to the referring physician's EHR as appropriate. The primary care physician's EHR system receives the patient-visit summary updates and incorporates data from them into the patient's record.

Provider Directory and Trust Framework Steps (elaboration on certain steps from Section 2)

1 **Query Individual Provider Directory**– Requesting Provider queries for the consulting specialist from whom she will request ongoing updates.

Query Provider's Associated Entities – selects the appropriate entity/location where the patient receives specialist care and where the patient's electronic record is maintained.

2 **Query Entity's Node Record and Services Information** – the EHR selects the Specialist's Node to receive the request and determines the supported protocols and payloads for the Subscription request.

7 **Verify Subscribing Entity Certificate** – upon receipt of the request, publishing physician's EHR verifies the requesting entity is trusted by Cal eConnect.

7 **Confirm Subscribing Entity** – specialist physician's EHR verifies the message is signed by the trusted entity

8 **Confirm Subscribing Provider** – specialist physician's EHR verifies the subscribing provider (in this case the primary care physician)

Provider Directory Entries:

ILPD	Providers (physicians, nurse practitioners, physician assistants), Departments
ELPD	Entities (hospitals, physician practices, clinics …) and Nodes for each

Services Registry: Supported protocols and payloads for the subscribe transaction

Questions:

1 Describe in detail how your proposed solution will meet the requirements for this use case. Please list all assumptions.

2 Describe which capabilities currently exist in your solution and which will need to be developed

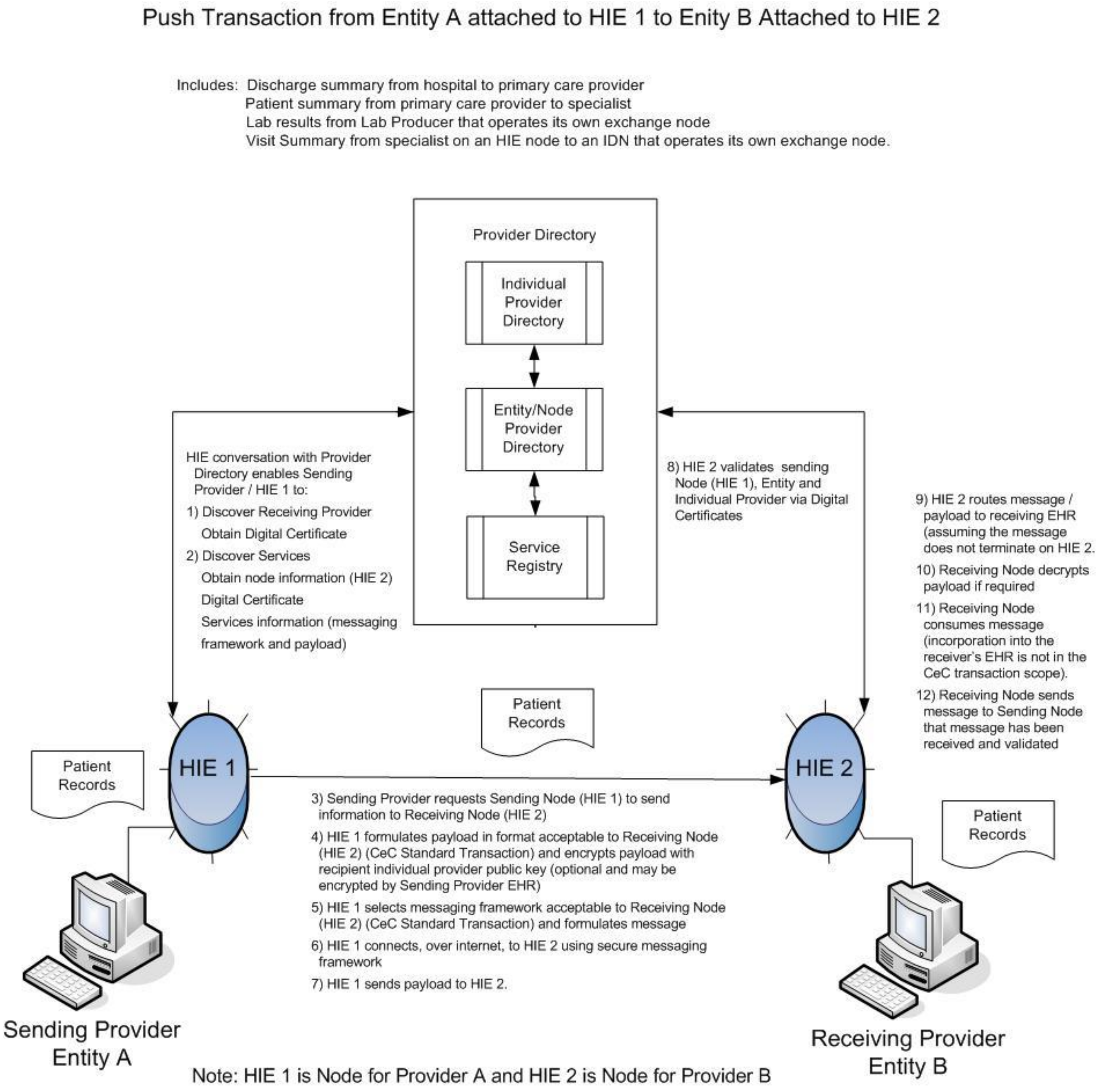
3 Describe the current capability of your solution to support multiple messaging standards that allow a "Publish-Subscribe" transaction. At a minimum describe you support for NwHIN Exchange, Direct Project, and the ability to create and support the framework described in Exhibit B.

4 Describe the additional artifacts and message types that will be needed by your solution to support the Publish-Subscribe transaction.

5 If a specific Sending EHR or Receiving EHR does not support a Publish-Subscribe transaction how do you propose that this transaction type be implemented?

6. Use Case 4: HIE to HIE Transaction – Primary care physician to specialist

General HIE to HIE Transaction:



Push Transaction from Entity A attached to HIE 1 to Enity B Attached to HIE 2

Includes: Discharge summary from hospital to primary care provider
Patient summary from primary care provider to specialist
Lab results from Lab Producer that operates its own exchange node
Visit Summary from specialist on an HIE node to an IDN that operates its own exchange node.

HIE conversation with Provider Directory enables Sending Provider / HIE 1 to:

1) Discover Receiving Provider
Obtain Digital Certificate

2) Discover Services
Obtain node information (HIE 2)
Digital Certificate
Services information (messaging framework and payload)

3) Sending Provider requests Sending Node (HIE 1) to send information to Receiving Node (HIE 2)

4) HIE 1 formulates payload in format acceptable to Receiving Node (HIE 2) (CeC Standard Transaction) and encrypts payload with recipient individual provider public key (optional and may be encrypted by Sending Provider EHR)

5) HIE 1 selects messaging framework acceptable to Receiving Node (HIE 2) (CeC Standard Transaction) and formulates message

6) HIE 1 connects, over internet, to HIE 2 using secure messaging framework

7) HIE 1 sends payload to HIE 2.

8) HIE 2 validates sending Node (HIE 1), Entity and Individual Provider via Digital Certificates

9) HIE 2 routes message / payload to receiving EHR (assuming the message does not terminate on HIE 2.

10) Receiving Node decrypts payload if required

11) Receiving Node consumes message (incorporation into the receiver's EHR is not in the CeC transaction scope).

12) Receiving Node sends message to Sending Node that message has been received and validated

Provider Directory
Individual Provider Directory
Entity/Node Provider Directory
Service Registry
Patient Records
HIE 1
HIE 2
Patient Records
Patient Records
Sending Provider Entity A
Receiving Provider Entity B

Note: HIE 1 is Node for Provider A and HIE 2 is Node for Provider B

Typical Story

A primary care provider using an EHR attached to an HIE (HIE-1) wishes to send a patient summary to a specialist whose EHR is connected to another HIE (HIE-2). The primary care provider uses HIE-1's access to the provider directory services with eHIE capabilities infrastructure to discover the physician, clinic location, and the information required to route the transaction through the associated HIE to the specialist's node. The patient summary (CCD) is sent from the primary care provider's EHR, via HIE-1 to HIE-2 and routed to the specialist's EHR at the relevant clinic location. The clinic's EHR system receives the CCD and incorporates the data from it into the patient's record.

Provider Directory and Trust Framework Steps (elaboration on certain steps from Section 2)

1. **Query Individual Provider** Directory– Primary care physician uses HIE-1's expanded physician look-up to query the provider directory services with eHIE capabilities infrastructure to find the desired specialist for the referral.

   Query Provider's Associated Entities – selects the appropriate entity/location where the patient receives specialty care and where the patient's electronic record is maintained.

2. **Query Entity's Node Record and Services Information** – selects the node (HIE-2) to receive the information and determines the supported protocols and payloads for the exchange of the patient summary.

7 **Verify Sending Entity Certificate** – HIE 2 verifies the sending entity is trusted by Cal eConnect.

7 **Confirm Sending Entity** – HIE 2 verifies the message is signed by the trusted entity

8 **Confirm Sending Provider** – HIE 2 verifies the sending provider (in this case the primary care physician)

Provider Directory Entries:

ILPD Providers (physicians, nurse practitioners, physician assistants), Departments

ELPD Entities (hospitals, physician practices, clinics …) and Nodes for each

Services Registry: Supported protocols and payloads for each transaction type

Questions:

1 Describe in detail how your proposed solution will meet the requirements for this use case. Please list all assumptions.

2 Describe which capabilities currently exist in your solution and which will need to be developed.

3 Please list all HIEs with which your solution currently has an interface.

4 What issues do you anticipate with this use case and the HIE-HIE interface described?

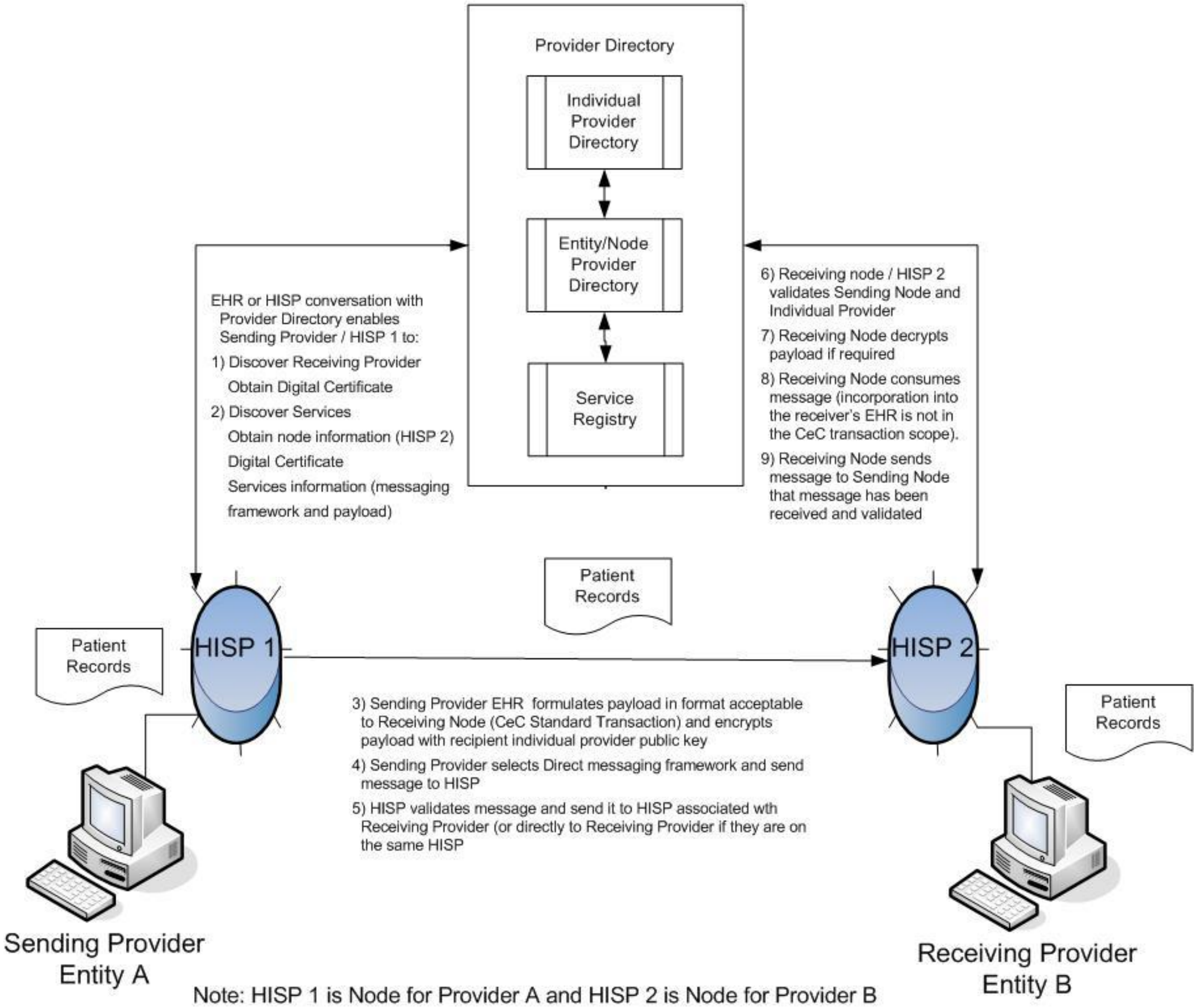
5 Suggest any alternatives that utilize the Provider Directories and accomplish the same secure transport of a clinical summary between HIEs.

7. *Use Case 5: HISP Transaction – Primary care physician to specialist*

General HISP Transaction:

Push Transaction from Entity A Utilizing HISP 1 to Enity B Utilizing HISP 2

Includes: Discharge summary from hospital to primary care provider
Patient summary from primary care provider to specialist
Lab results from Lab Producer that operates its own exchange node
Visit Summary from specialist on an HIE node to an IDN that operates its own exchange node.


Provider Directory
Individual Provider Directory
Entity/Node Provider Directory
Service Registry
Patient Records
HISP 1
HISP 2
Patient Records
Patient Records
Sending Provider Entity A
Receiving Provider Entity B

EHR or HISP conversation with Provider Directory enables Sending Provider / HISP 1 to:

1) Discover Receiving Provider
Obtain Digital Certificate

2) Discover Services
Obtain node information (HISP 2)
Digital Certificate
Services information (messaging framework and payload)

3) Sending Provider EHR formulates payload in format acceptable to Receiving Node (CeC Standard Transaction) and encrypts payload with recipient individual provider public key

4) Sending Provider selects Direct messaging framework and send message to HISP

5) HISP validates message and send it to HISP associated wth Receiving Provider (or directly to Receiving Provider if they are on the same HISP

6) Receiving node / HISP 2 validates Sending Node and Individual Provider

7) Receiving Node decrypts payload if required

8) Receiving Node consumes message (incorporation into the receiver's EHR is not in the CeC transaction scope).

9) Receiving Node sends message to Sending Node that message has been received and validated

Note: HISP 1 is Node for Provider A and HISP 2 is Node for Provider B

Typical Story

A primary care provider using an EHR supporting the Direct Project messaging framework utilizes a CeC-certified HISP to send a patient summary to a specialist whose EHR also supports the Direct Project messaging framework and is connected to another CeC-certified HISP. The primary care provider uses his EHR's or HISP's access to the provider directory services with eHIE capabilities infrastructure to discover the physician, clinic location, and the information required to route the transaction to the specialist. The patient summary (CCD) is sent from the primary care provider's EHR, via HISP-1 to HISP-2 and routed to the specialist's EHR at the relevant clinic location. The receiving provider's EHR system receives the CCD and incorporates the data from it into the patient's record.

Provider Directory and Trust Framework Steps (elaboration on certain above steps)

1 **Query Individual Provider** Directory – Primary care physician uses the capability of his EHR or HISP to query Cal eConnect provider directory services with eHIE capabilities infrastructure to find the desired specialist for the referral.

Query Provider's Associated Entities – selects the appropriate entity/location where the patient receives specialty care and where the patient's electronic record is maintained.

2 **Query Entity's Node Record and Services Information** – selects the node HISP-2 to receive the information and determines the supported Direct protocols and payloads for the exchange of the patient summary.

7 **Verify Sending Entity Certificate** – HISP 2 (or the receiving EHR) verifies the sending entity is trusted by Cal eConnect.

7 **Confirm Sending Entity** – HISP 2 (or the receiving EHR) verifies the message is signed by the trusted entity

8 **Confirm Sending Provider** – HISP 2 (or the receiving EHR) verifies the sending provider (in this case the primary care physician)

Provider Directory Entries:

ILPD Providers (physicians, nurse practitioners, physician assistants), Departments

ELPD Entities (hospitals, physician practices, clinics …) and Nodes for each

Services Registry: Supported protocols and payloads for Direct Messaging

Questions:

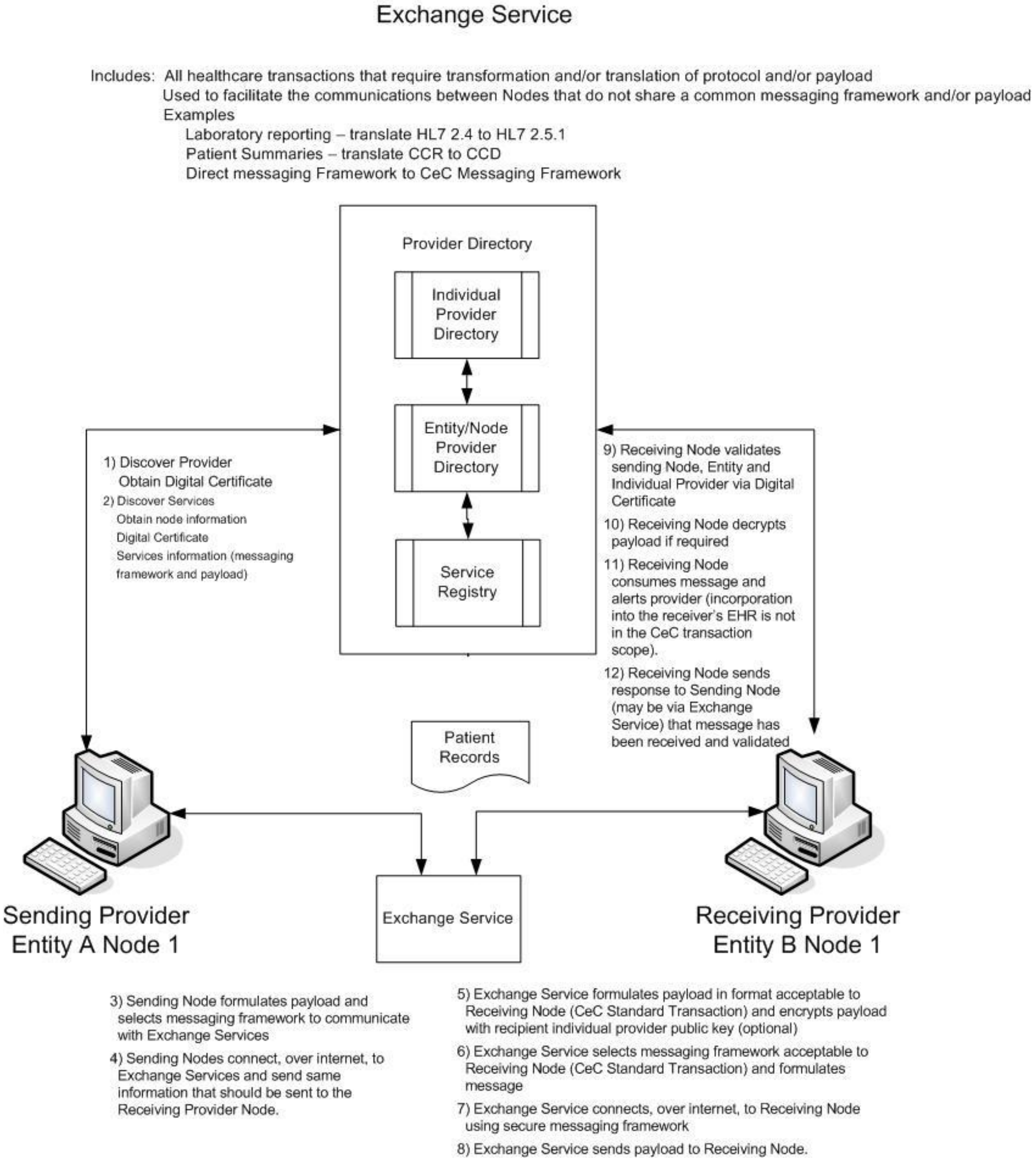
1. Describe in detail how your proposed solution will meet the requirements for this use case. Please list all assumptions.
2. Describe which capabilities currently exist in your solution and which will need to be developed. Include your capability and experience supporting the Direct Project protocol (including as a HISP).
3. Please list all HISPs with which your solution currently communicates or which your solution is in the process of supporting and the status of each such implementation.

4. What issues do you anticipate with this use case and the HISP-HISP interface described?

5. If the sending or receiving physician’s EHR does not support the Direct Protocol, how do you propose that the primary care physician communicate a patient summary to the specialist?

8. Use Case 6: Exchange Services -- Hospital Discharge Summary to Clinician

General Exchange Service Transaction:



Exchange Service

Includes: All healthcare transactions that require transformation and/or translation of protocol and/or payload
Used to facilitate the communications between Nodes that do not share a common messaging framework and/or payload
Examples
Laboratory reporting – translate HL7 2.4 to HL7 2.5.1
Patient Summaries – translate CCR to CCD
Direct messaging Framework to CeC Messaging Framework

Provider Directory
Individual Provider Directory
Entity/Node Provider Directory
Service Registry
Patient Records
Exchange Service
Sending Provider Entity A Node 1
Receiving Provider Entity B Node 1

1) Discover Provider
Obtain Digital Certificate

2) Discover Services
Obtain node information
Digital Certificate
Services information (messaging framework and payload)

3) Sending Node formulates payload and selects messaging framework to communicate with Exchange Services

4) Sending Nodes connect, over internet, to Exchange Services and send same information that should be sent to the Receiving Provider Node.

5) Exchange Service formulates payload in format acceptable to Receiving Node (CeC Standard Transaction) and encrypts payload with recipient individual provider public key (optional)

6) Exchange Service selects messaging framework acceptable to Receiving Node (CeC Standard Transaction) and formulates message

7) Exchange Service connects, over internet, to Receiving Node using secure messaging framework

8) Exchange Service sends payload to Receiving Node.

9) Receiving Node validates sending Node, Entity and Individual Provider via Digital Certificate

10) Receiving Node decrypts payload if required

11) Receiving Node consumes message and alerts provider (incorporation into the receiver's EHR is not in the CeC transaction scope).

12) Receiving Node sends response to Sending Node (may be via Exchange Service) that message has been received and validated

Typical Story

A hospital discharge summary is sent from a hospital EHR to a primary care physician's EHR at the relevant practice location. The hospital EHR uses an Exchange Service to convert the patient discharge summary from a CCR format to a CCD format, because the latter is required by the practice's EHR system, but the hospital EHR cannot produce a CCD document. The clinic's EHR system receives the converted discharge summary and incorporates data from it into the patient's record.

Provider Directory and Trust Framework Steps (elaboration on certain steps from Section 2)

1 **Query Individual Provider Directory**– Sending Provider queries for the desired outpatient Provider to receive the discharge summary.

Query Provider's Associated Entities – selects the appropriate entity/location where the patient receives primary care and where the patient's electronic record is maintained.

2 **Query Entity's Node Record and Services Information** – selects the Node to receive the information and determines the supported protocols and payloads for the exchange of a discharge summary and determines that the use of an Exchange Service is required to support the CCD payload.

7 **Verify Sending Entity Certificate** – physician's EHR verifies the sending entity is trusted by Cal eConnect (this may be the Exchange Services as a proxy for the sending entity.

7 **Confirm Sending Entity** – physician's EHR verifies the message is signed by the trusted entity

8 **Confirm Sending Provider** – physician's EHR verifies the sending provider (in this case the responsible physician at the hospital)

Provider Directory Entries:

ILPD	Providers (physicians, nurse practitioners, physician assistants), Departments
ELPD	Entities (hospitals, physician practices, clinics …) and Nodes for each

Services Registry: Supported protocols and payloads for each transaction type

Exchange Services – if the sender does not support the necessary protocol and payload standards, it may utilize an Exchange Service to act as a proxy and translate the message and payload to the correct format for the recipient.

Questions:

1. Describe in detail how your proposed solution will meet the requirements for this use case. Please list all assumptions.
2. Describe which capabilities currently exist in your solution and which will need to be developed

3. Describe the current capability of your solution to transform message types to allow communication between EMRs supporting different standards.

4. Describe the security and authorization artifacts and message types that will be needed by your solution to support the Exchange transaction(s).

5. What issues do you anticipate in providing the Exchange Services?

   a. Converting payload messaging formats

   b. Converting transport and security protocols

   c. Converting payload clinical terminologies

6. If a Sending EHR or Receiving EHR does not support any of the messaging frameworks (NwHIN Exchange, Direct Project, Cal eConnect Messaging Framework) how will your solution support the communication of patient information between these EHRs?

7. Please list all Immunization registries and departments of public health with which your solution currently exchanges information electronically and the protocols it supports to do so.

8. Since one of the possible uses of these transactions is communication with health plans to enable various X.12 transactions, please list the health plans with which your solution currently exchanges information in an X.12 format and the specific X.12 transactions supported

9. Use Case 7: California Medicare Advantage Payers

Background

Medicare Advantage payers are frequently required by CMS to retrieve “signed / credentialed” medical records for member encounters (from physicians) or in-patient stays (from hospitals).

Currently, these records are retrieved at considerable expense in the following ways:

a. Manually (copies, scans or faxes obtained directly from the provider/hospital by mail, email or in person)

b. Digitally (as .pdf files made available by record retrieval vendors (i.e. MediConnect Global) or by 3rd-party EDI vendors, i.e. HealthPort.)

c. EDI channel direct from large hospitals to large payers (i.e. UnitedHealth / Ingenix)

Data in these records usually needs to be re-keyed in order for it to become part of the payer’s workflow systems. The process is time-consuming and open to many errors (keying, copying, etc.)

Use Case Questions

1. How could Medicare Advantage payers use Cal eConnect’s service to request and receive data from provider or hospital EMR/EHR systems?

2. Since payers don’t have EHR systems, what interface would be required at their end to send and receive data?

3. What opportunities might exist for batch requests (i.e. in-patient records with various Dates of Service (DOS) for one member, or cumulative records for various members from one physician/provider)?

ATTACHMENT A – MINIMUM CORPORATE EXPERIENCE SUMMARY FORM

Bidder's Name:	**Today's Date:**
Number of Years in Business (minimum of 5):	

Health Care Clients (minimum of 6)		
	Client Name	**Inter-Enterprise Exchange Using Provider Directory? (Y/N)** **(minimum of 1 "Yes")**
1.		
2.		
3.		
4.		
5.		
6.		

Health Information Exchange Via Public Internet (minimum of 3 client projects)			
	Client Name	**Number of External Users**	**Number of Transactions per Year**
1.			
2.			
3.			

Other Experience	
1.	**Describe your consortium's familiarity with HITECH, the ONC, CMS' EHR Incentive Program and the Meaningful Use Criteria, NwHIN and related standards, etc.**
2.	**Describe your consortium's technical and functional knowledge of HIT data representation, transport protocols, directory services, trusts frameworks, & related standards/methods.**
3.	**Describe your consortium's experience with large-scale transaction-based systems that displays the capability to ensure flexibility and scalability.**
4.	**Describe your consortium's experience hosting and operating a web services solution in compliance with HIPAA security controls.**
5.	**Describe your consortium's experience providing support (including help desk and technical on-boarding) to a large number of users and organizations.**

ATTACHMENT B – CORPORATE EXPERIENCE CLIENT REFERENCE FORM

Bidder's Name:		**Today's Date:**
Referenced Project Name:		
Reference Name:		**Health Care Client? (Y/N):**
Address:		**Contact:**
		Telephone:
Email:		**FAX:**
Project Performance		
Project Start Date:		
Planned Completion Date:		**Explain Difference:**
Actual Completion Date:		
Planned Cost:		**Explain Difference:**
Actual Cost:		
Did Solution Include a Provider Directory?:		**Number of Providers in System:**
Did You Host & Maintain Solution for Client?:		**Volume of Transactions Processed per Month:**
Number of Users: • **Internal to Client:** • **External to Client:**		**HIE Product(s) Implemented (if applicable):**
Did Solution Exchange Information via the public internet, appropriate security and access-control techniques?:		
Did Solution Comply with HIPAA Security Controls?:		
Brief Description of Project (include description of hosting and operations services, if appropriate):		

ATTACHMENT C – PROJECT TEAM FORM

Title	Name	Role	Responsibilities	Percentage of time on project
		Project Manager		

ATTACHMENT D – MINIMUM STAFF EXPERIENCE FORM

Qualification	Staff Name & Role	Response
1. The Proposed Project Manager must be currently certified by the Project Management Institute as a Project Management Professional. Provide PMP certification number.	Project Manager	
2. Minimum of 5 years' experience designing, developing, and implementing IT solutions		
3. Experience with at least 1 client project with inter-enterprise exchange among diverse partners using a provider directory		
4. Experience with at least 1 client project that implemented systems to exchange health information among independent organizations via the public internet and appropriate security and access-control techniques. The systems must be or have been in production with at least 200 users or 5,000 transactions/year		

ATTACHMENT E – PRE-EXISTING SOFTWARE FORM

Use the form below to itemize the Contractor, open source, or other licensed third-party pre-existing software that will be used in the Contractor's solution, including development, test, training and other support tools. Where Bidder's proposed solution utilizes licensed products that may constrain Cal eConnect Policy decisions, use additional pages to indicate what terms may need negotiation prior to release.

#	Item Description/ Purpose	Manufacturer/ Product Name	Version	Licensing Model (e.g., per seat, per server, view only, developer, open source)	Number of Licenses Provided
1					
2					
3					
4					

ATTACHMENT F – COST PROPOSAL INSTRUCTIONS AND FORMS

The Bidder must follow the instructions below for the completion of their cost proposal. The cost proposal forms are documented in an Excel workbook named “Provider Directory RFP Cost Proposal Template.xlsx.” All prices given must be complete and inclusive, providing details for all ancillary costs including taxes, management, oversight, document or media copying, and travel expenses. All cost information must be separately sealed and identified as indicated in Section IV.G, Proposal Packaging and Delivery.

1. **Two-Year Summary Worksheet**
   - Provide cost estimates for each of the service categories described in Sections III.A and III.C using the columns provided in the worksheet.
   - Provide cost estimate summaries in each cost category for one-time costs, and ongoing costs for years one and two.
   - Provide separate summaries for each III.A.11 Exchange Service Capability category
     - Framework – All costs associated with setting up exchange services, with the exception of the costs related to specific protocols.
     - Laboratory Results – Costs related to exchange services for the laboratory results protocol.
     - Patient Summaries – Costs related to exchange services for the patient summaries protocol.
   - The two-year total cost on this worksheet will be the basis for the evaluation of the Bidder’s Cost Proposal, as described in Section V.B.3.
   - Do not include costs related to the Optional Value-Add Exchange Services and Approach to Sustainability described in Section IV.E in this Two-Year Summary Worksheet. These costs should be accounted for as described in Item 5 below.
2. **One-Time Cost Worksheets**
   - One-Time Cost - Labor Detail Tab: Provide an estimate of one-time professional services costs by task/deliverable. The hourly labor rates provided in this table will be used for work authorizations for additional work as described in Section VI.
   - One-Time Cost - Software Detail Tab: Provide any one-time licensing costs for software. Explain the licensing fee structure including pricing model, assumptions, and other relevant licensing information.
   - One-Time Cost - Data Center Detail Tab: Provide any one-time costs related to data center hosting services, such as hardware or telecommunications costs.
   - One-Time Cost - Other Detail Tab: Provide other one-time costs, as needed, to provide a complete cost picture for the service. Provide a description of any other costs included.

- Do not include costs related to the Optional Value-Add Exchange Services and Approach to Sustainability described in Section IV.E in the one-time cost worksheets. These costs should be accounted for as described in Item 5 below.

3. **Ongoing Cost Worksheets**

- Ongoing Cost - Labor Detail Tab: Provide an estimate of ongoing professional services costs by task/deliverable for years one and two. The hourly labor rates provided in this table will be used for work authorizations for additional work as described in Section VI.
- Ongoing Cost - Software Detail Tab: Provide any ongoing licensing maintenance/support costs for software for years one and two.
- Ongoing Cost - Data Center Detail Tab: Provide any ongoing costs related to data center hosting services, such as hardware or telecommunications costs, for years one and two.
- Ongoing Cost - Other Detail Tab: Provide other ongoing costs, as needed, to provide a complete cost picture for the service for years one and two. Provide a description of any other costs included.
- Include applicable costs for participating trading partners in the relevant cost item (e.g. licensing fee, setup fees, transaction costs, maintenance, etc.).
- Do not include costs related to the Optional Value-Add Exchange Services and Approach to Sustainability described in Section IV.E in the ongoing costs worksheets. These costs should be accounted for as described in Item 5 below.

4. **Deductions for Reduced Scope Options**

- Use additional pages to describe the deduction from the full service cost to provide the reduced services as described in Section IV.C Proposed Approach to the Scope of Work:
    - Provide amount to be deducted from the IV.C.1, Item 2, Hosting and Data Center Operations, full service cost, assuming the solution is hosted at a third-party facility and the Bidder provides maintenance and operations services.
    - Provide the amount to be deducted from the IV.C.1, Item 5, Provider Certification and Maintenance, full service cost, assuming the Bidder provides intermediate credentialing services instead of CVO services.
    - Provide the amount to be deducted from the IV.C.1, Item 5, Provider Certification and Maintenance, full service cost, assuming the Bidder provides no credentialing services. Credentialing is performed by Cal eConnect or another party.
    - Provide the amount to be deducted from the IV.C.1, Item 10, Billing and Accounts Receivable Services, full service cost, assuming the Bidder only provides the data necessary to perform billing activities and billing and accounts receivable activities are performed by Cal eConnect or a third party.

5. Cost Estimates for Optional Exchange Services

- Use the Excel workbook named “Provider Directory RFP Cost Proposal Optional Services.xlsx” file to document the costs for the Bidder’s proposed Optional Value-Add Exchange Services and Approach to Sustainability described in Section IV.E. Create a separate copy of this Excel workbook for every optional service described.
- All tabs labeled “Optional” should be completed using the same instructions as described in Items 1, 2, and 3 above for the Bidder’s proposed optional exchange services.
- These costs will not be used in the calculation of the Bidder’s cost proposal score. However, these costs may be used as the basis for discussion and bargaining during interviews or subsequent negotiation.

6. Assumptions

- Use additional pages to describe assumptions used to calculate costs, by service/task and cost category. Include description and rationale for the basis of calculation (e.g., labor hours, transactions, support calls, etc.).

7. Alternative Cost Estimates

- Use additional pages to describe alternative financing models (e.g. low/no upfront cost, ongoing monthly fees, transaction-based models, risk-sharing models) that favor the long-term sustainability of the infrastructure. Provide an additional cost estimate template for each alternative model.
- Bidders should also provide recommendations or changes to scope, functionality, or assumptions that would result in a reduced cost estimate, and the amount of the cost reduction.

[i] See http://www.ws-i.org/Profiles/BasicProfile-2_0(WGD).html for detailed technical specifications.

[ii] See http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html for detailed technical specifications.

[iii] See http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_910523_0_0_18/NHIN_MessagingPlatformProductionSpecification_v2.0.pdf for detailed specifications of the NwHIN Messaging Platform.

[iv] See http://edocket.access.gpo.gov/2010/pdf/2010-17210.pdf

[v] See http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_11673_910545_0_0_18/NHIN_AuthorizationFrameworkProductionSpecification_v2.0.pdf

[vi] See http://www.ietf.org/rfc/rfc3280.txt